Sale viernes sí, viernes no • PRÁCTICA • ACTUAL • QUINCENAL

Computer Hoy

Nº 701 • AÑO XXVII
DEL 14 AL 28 DE AGOSTO DE 2025
computerhoy.com

Menores y grupos de WhatsApp

actualidad

¡Peligro a la vista!

Todas las amenazas de Internet

- Supersticiones y riesgos digitales: **5 falsos mitos de seguridad**
- Servicios y apps de EE. UU.: ¿**son fiables**? Las alternativas europeas
- **Así clonan con IA** la voz de tus amigos y familiares
- **Nueva estafa:** 'Su paquete no ha podido ser entregado'

VERSIÓN ACTUALIZADA 2025

test

COMPARATIVA

10 Suites de seguridad

- ¿**Cuánto cuesta** proteger tus dispositivos?
- ¿Es suficiente con una **solución gratuita**?
- ¿Qué **protección extra** ofrece una de pago?
- ¿En qué hay que **fijarse antes de comprar**?

10 Servicios VPN analizados en el laboratorio

¿Cuál es el mejor para **navegar seguro** en Internet?

EXTRA SEGURIDAD

TODO LO QUE DEBES SABER PARA ESTAR PROTEGIDO

práctico

Cuentas temporales

Emails de usar y tirar

Seguridad y privacidad

¿Están tus datos en la Dark Web?

Los mejores trucos de control parental

Comprobación de archivos

Descargas seguras desde Internet

saber más

Criptografía y computación

¿Es seguro almacenar nuestra vida en la nube?

Las primeras 24 horas en un hipotético corte global de Internet

KIOSKEROS

Computer Hoy

unclick

La newsletter de **Computer Hoy**

La tecnología desde un punto de vista muy personal

Suscríbete a nuestra newsletter gratuita, donde nuestros expertos te contarán la actualidad tecnológica de una forma diferente.

Suscríbete aquí

EDITORIAL

Computer Hoy Nº 701

CARLOS GOMBAU
Redactor Jefe

LA SEGURIDAD ES UNA ASIGNATURA PENDIENTE EN ORDENADOR Y MÓVIL

"Tranquilo, que yo controlo", pero no... Por quinto año consecutivo, un verano más te traemos un número especial con los mejores artículos sobre seguridad publicados en las páginas de Computer Hoy durante los últimos 12 meses. En la primera edición, hace cuatro años, apelaba en esta misma página a la Teoría de Compensación del Riesgo para explicar cómo el exceso de confianza nos lleva a no tomar las medidas de precaución necesarias ante escenarios de peligro. Como comentaba, la teoría se conoce actualmente como efecto Peltzman y afirma que, cuanto menor es el riesgo percibido en una situación determinada, las medidas de precaución que tomamos son menores. O, dicho de otra forma, tenemos comportamientos más o menos arriesgados en función de si nos sentimos más o menos protegidos. Y luego vienen los sustos.

Compensamos las medidas de seguridad impuestas tomando conductas más atrevidas de lo normal. El problema es que este sentir puede ser solo una mera ilusión. Recuerda, los sesgos cognitivos se alimentan de nuestra ignorancia sobre ellos: que no percibamos el riesgo o que nos sintamos seguros, no quiere decir que no exista. En este sentido, el Instituto Nacional de Ciberseguridad (INCIBE) junto al Observatorio Nacional de Tecnología y Sociedad (ONTSI) publicaron en agosto de 2024 un nuevo dosier 'Cómo se protege la ciudadanía ante los ciberriesgos', un estudio sobre la percepción y el nivel de confianza en España en seguridad informática.

> "EL 50 % DE LOS USUARIOS QUE SE CONSIDERAN PREPARADOS TIENE SUS EQUIPOS INFECTADOS".

Entre otras cifras y conclusiones que merece la pena analizar, destaca que muchos usuarios de PC creen tomar medidas de seguridad, cuando en realidad no son conscientes de que no (el 45,8 % cree tener su sistema actualizado, cuando sus dispositivos reflejan que el 39,5 % lo está). A esto se suma que afirman adoptar medidas de privacidad, pero la realidad lo desmiente. En el hogar, se tiende a pensar que los PC son más seguros de lo que son, mientras que los móviles se perciben como más vulnerables de lo que han demostrado ser. Solo un dato más: el 50 % de los usuarios que se consideran totalmente preparados en ciberseguridad tiene sus equipos infectados. El riesgo es real.

carlos.gombau@henneo.com | **@cgombau**

Tu opinión cuenta...

Computer Hoy computerhoy.com | ComputerHoy | @computerhoy | ComputerhoyTV | @computerhoy.com | store HENNEO www.henneomagazines.com

No te pierdas...

EL FUTURO DIGITAL: NUEVAS AMENAZAS

Malware, robo d e información, fraude... Internet no es solo diversión, sino también un patio de recreo para los estafadores. Te explicamos qué amenazas acechan y cómo puedes protegerte. **Página 6**

CORREO TEMPORAL EN SEGUNDOS

El correo de usar y tirar evita el spam y protege tu privacidad al registrarte online. Se crea fácilmente y se elimina tras un tiempo, sin ocupar almacenamiento. **Página 36**

¿CUÁL ES EL MEJOR ANTIVIRUS PARA TI?

Con el aumento de las amenazas como malware, phishing y fraudes online, contar con un software que sea fiable y completo es realmente esencial en el mundo digital actual. **Página 48**

SUMARIO

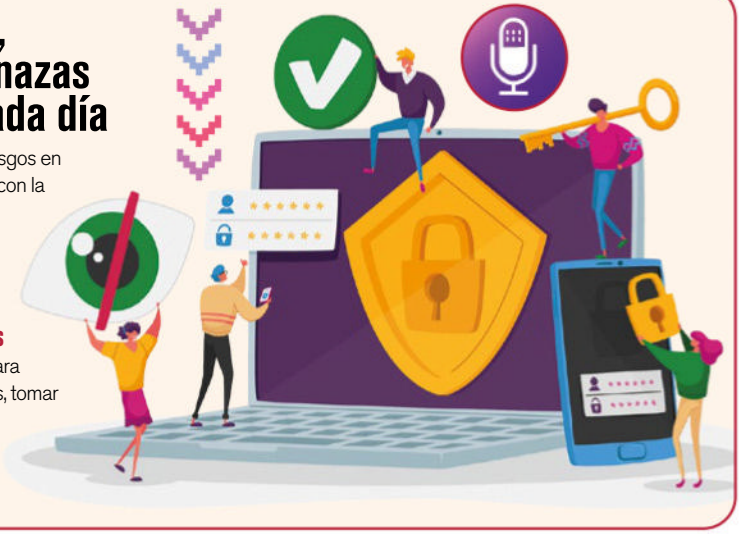
COMPUTER HOY Nº 701

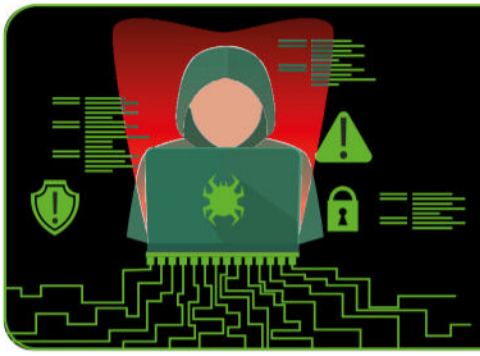
6 Internet, las amenazas aumentan cada día

Según los expertos, los riesgos en Internet siguen creciendo con la inteligencia artificial, exponiendo a usuarios a fraudes, virus, phishing y robo de identidad.

Identificar las amenazas

Te ofrecemos las claves para reconocer riesgos digitales, tomar precauciones efectivas y mantener tu seguridad personal frente a posibles ataques.





36 La seguridad está en tus manos

Proteger tu privacidad es cada vez más importante. Por ello, en la página 36 te explicamos cómo crear emails temporales para evitar el spam y mantener la privacidad.

Protección familiar y filtración de datos

Pero ahí no queda todo. En la sección de artículos prácticos, te ayudamos a controlar la actividad online de tus hijos y a descubrir si tus datos están en la Dark Web.

48 Más que un antivirus: seguridad para tu vida digital

Hoy en día, un antivirus básico no es suficiente para hacer frente a todas las amenazas actuales. Los paquetes de seguridad completos incluyen herramientas como VPN, gestor de contraseñas y protección de identidad. Nosotros hemos evaluado cuidadosamente cada solución disponible en el mercado para ayudarte a elegir la mejor opción.

62 Desafíos del mundo digital

En nuestra sección 'Saber más', encuentras siempre interesantes artículos que amplían y explican los temas tecnológicos actuales. En esta ocasión, exploramos los desafíos y soluciones más urgentes del mundo digital. Por ejemplo, la seguridad en la nube se ha vuelto esencial para proteger datos sensibles. Al mismo tiempo, la falta de control parental deja a niños y adolescentes vulnerables en entornos digitales.

Actualidad

Todo sobre seguridad:
- Peligros online en 2025 6
- Cinco falsos mitos sobre ciberseguridad 8
- Esto no es seguro 10
- Alternativas a los servicios estadounidenses 12
- Llegan los DNS de la UE 14
- Así de fácil pueden los hackers descifrar tus contraseñas 16
- Vulnerabilidad de seguridad en los routers 18
- El peligro de los deepfakes 20
- Clonan con IA la voz de tus seres queridos 22
- Chantaje, ¡con fotos de IA! 24
- ¿Puede entrar tu smartphone en EE. UU.? 26
- Este cable te espía 28
- El coche en el punto de mira de los hackers 30
- Cuidado, suplantación de empresas de logística 32
- Delgado por 90 euros 34

Práctico

Correos desechables: Cómo crear un correo temporal para registrarte sin riesgos 36
Seguridad y privacidad: ¿Están tus datos personales en la Dark Web? 40
Google Fotos: Carpeta privada 43
Niños, pantallas y protección: Consejos para lograr mejorar el control parental 44
Descargas seguras: Comprobar si un archivo de Internet es seguro 46

Test

10 Suites de seguridad: Lo mejor contra los virus 2025 48
10 Servicios VPN: ¿En Internet y a salvo? 56

Saber más

Tecnología para todos:
- ¿Es seguro almacenar nuestra vida en la nube? 62
- Las apps comparten nuestros datos privados sin que lo sepamos 64
- Las primeras 24 horas en un hipotético corte global de Internet 66
- La curiosa razón por la que llamamos parches a las correcciones de bugs 68
- Niños y grupos de WhatsApp 70
- Cosas que jamás deberías buscar en Google 73

En el próximo número 74

La revista de videojuegos número 1 en España

Todos los meses en tu quiosco llena de reportajes, análisis, avances y mucho más. Contenidos exclusivos que no vas a encontrar en otra parte. **¡Corre a por ella!**

Consíguela aquí:

UNA PUBLICACIÓN DE
HENNEO MAGAZINES

KIOSKEROS

PELIGROS A LA VISTA 2025

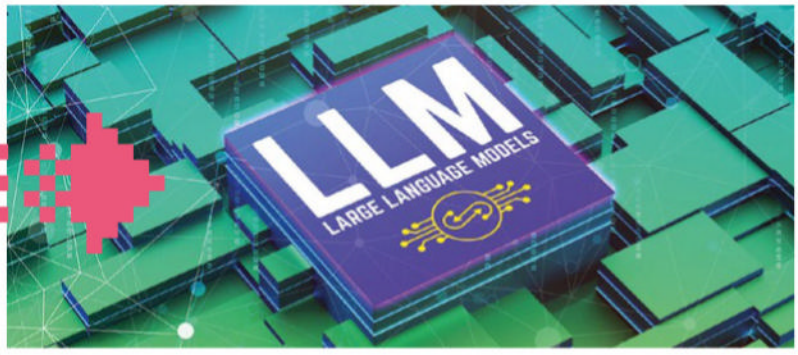
Internet será aún más peligroso en 2025, así que Computer Hoy te avanza qué puedes esperar.

> 2025 será un año de cambios, y será más importante que nunca proteger nuestra vida digital.
>
> **Siggi Stefnisson**
> CTO de Ciberseguridad en Gen

Malware, robo de datos, fraude... Internet no es solo diversión, sino también un patio de recreo para los delincuentes. Aún hoy, muchas personas siguen cayendo en los viejos métodos de estafa, pero **ni los internautas experimentados están a salvo**: los ciberdelincuentes desarrollan y perfeccionan constantemente sus artes oscuras. Gen, fabricante de Norton, Avira, Avast y otras soluciones de seguridad te explica aquí qué nuevas amenazas habrá en 2025 y cómo puedes protegerte. "Tras un año monumental para la IA –y un año bastante desastroso en términos de filtraciones de datos–, esperamos cambios significativos tanto en las estafas como en los riesgos de la identidad digital en 2025", afirma Siggi Stefnisson, CTO de Ciberseguridad en Gen. "Los ciberdelincuentes utilizarán las **filtraciones de datos para robar identidades** directamente o para utilizar la información en estafas hiperpersonalizadas y creíbles. La IA agrava los problemas, no solo ayudando a los delincuentes a perfeccionar sus ataques, sino también obligando a la gente a cuestionarse cómo influye la tecnología en el pensamiento humano". Esto significa que la protección es más importante que nunca. Sin embargo, también quiere decir que, aunque un programa antivirus es una buena base, por sí solo difícilmente bastará para mantenerte a salvo y repeler todos los ataques. Sigue leyendo para saber qué puedes esperar este año y qué **medidas deberías tomar** para poder protegerte mejor.

LA IA DIFUMINA LOS LÍMITES DE LA REALIDAD COTIDIANA Y EVIDENCIA ALGUNOS RIESGOS

La inteligencia artificial está en alza y se utiliza cada vez más y en más ámbitos. A finales del pasado 2024, más de 200 millones de personas ya utilizaban cada semana ChatGPT y, por supuesto, esta tendencia continuará y crecerá en 2025. Sin embargo, el uso de la IA no siempre está exento de riesgos. Porque, aunque parezca lo contrario, las inteligencias artificiales no tienen sentimientos, ni moral, ni conciencia. Sin reglas, una IA también ayuda a construir bombas, planear atentados, chantajear o presentar contenidos inapropiados a los niños, por ejemplo. En consecuencia, la Unión Europea y varios estados de EE. UU. ya han introducido leyes para regular el uso de las IA. Hay que reconocer, sin embargo, que debido al rápido desarrollo de las aplicaciones de inteligencia artificial, cada vez es más difícil reaccionar con rapidez.



DEEPFAKES DIFÍCILMENTE RECONOCIBLES

La IA avanza tanto que incluso los expertos ya no reconocen qué es auténtico. Cada vez más personas deben cuestionar la autenticidad de las imágenes y vídeos, ya sea frente a una expareja descontenta que difunde rumores en las redes sociales o gobiernos que manipulan a poblaciones enteras publicando vídeos cargados de desinformación política. El engaño es cada vez más sofisticado: se necesitan pruebas digitales fiables para demostrar que una foto, un vídeo, una llamada telefónica, un mensaje de voz o incluso un correo electrónico son auténticos. Usando como plantilla la voz de un vídeo o publicación de Facebook, es posible generar nuevas frases y, con el tiempo, esta manipulación podría realizarse incluso en tiempo real.

LAS FILTRACIONES DE DATOS **ROBAN IDENTIDADES**

Desde Banco Santander a Ticketmaster, el 2024 se caracterizó por muchas filtraciones de datos. Los ciberdelincuentes aprovechan la información de los clientes de estas empresas para crear identidades falsas, completándolas con datos de fuentes públicas como Facebook y otras plataformas. Luego, suplantan a las víctimas y utilizan sus datos para todo tipo de ataques. Por ejemplo, pueden hacerse pasar por los empleados de una empresa, para ordenar transferencias de dinero, o ejecutar sofisticados intentos de chantaje dentro del círculo cercano de la persona afectada.

ROBOS FINANCIEROS CON NUEVO ASPECTO

En 2025 se producirá un fuerte aumento de los ataques a nuestras finanzas. Los ciberdelincuentes centrarán sus esfuerzos sobre todo en la banca móvil y aprovecharán el creciente atractivo de las criptomonedas, atrayendo a quienes sueñan con ganar dinero rápido y terminan conectando con estafadores en Internet. En los vídeos deepfakes, personajes famosos prometen grandes beneficios en oscuras plataformas de inversión. La campaña CryptoCore de 2024, por ejemplo, funcionó con un deepfake de Elon Musk y provocó pérdidas millonarias, ya que el dinero invertido por las incautas víctimas desapareció. Habrá más de esto en 2025 y, para colmo, la ciberdelincuencia se entrelazará cada vez más con la delincuencia callejera ordinaria, obligando a las víctimas a desbloquear sus teléfonos para acceder a sus aplicaciones financieras.

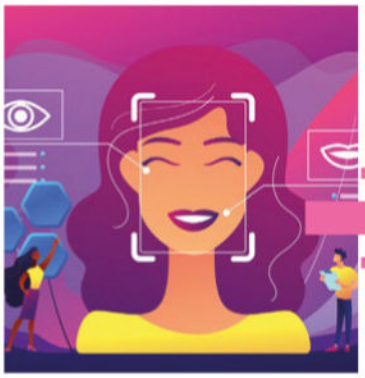
CÓMO **PROTEGERTE**

Los siguientes consejos te ayudarán a prepararte de una forma óptima, para de esta forma no caer ante las nuevas amenazas:

- **Mantente informado:** sigue las noticias y mantente siempre al tanto de las últimas estafas y filtraciones de datos masivas.
- **Navega con seguridad:** utiliza una VPN para mantener a buen recaudo tus datos y tu información personal en Internet.
- **Mantente escéptico:** si algo parece demasiado bueno para ser verdad, suele deberse a que no es verdad. Piensa antes de hacer clic en los enlaces o de compartir información en línea.
- **Compruébalo dos veces:** antes de hacer clic en un enlace o compartir tus datos personales o bancarios, comprueba primero que el destinatario es realmente quien asegura ser.
- **Utiliza herramientas de seguridad fiables:** una solución de seguridad todo-en-uno te protege al mismo tiempo del malware, el espionaje, los enlaces maliciosos y reconocerá los sitios web falsos. Un programa así es imprescindible en cualquier dispositivo.
- **Protégete por partida doble:** siempre que sea posible, utiliza la autenticación de dos factores para iniciar sesión en tus cuentas.
- **Estate preparado:** reúne los contactos de emergencia y las claves más importantes y tenlo todo a mano en un lugar seguro para, llegado el caso, poder recuperar los cargos adeudados en las tarjetas de crédito, bloquear el acceso a las mismas o restablecer las contraseñas más delicadas si estás siendo atacado.

EL FRAUDE SE ADAPTA AL **PERFIL INDIVIDUAL** DE CADA UNA DE LAS VÍCTIMAS

¿Ataques a través de la brecha de seguridad de un software desactualizado? Eso era en el pasado. Los ciberdelincuentes se centran cada vez más en estafar a sus víctimas con trucos psicológicos. Los mensajes que parecen proceder de un amigo o las llamadas sobre supuestas emergencias que aparentan ser de familiares nos hacen bajar la guardia y transferir dinero de buena fe. Los información personal que utilizan los delincuentes para hacer esto se obtiene de filtraciones de datos y de la dark web. En otras palabras, los ataques son cada vez más selectivos y no llegan en forma de correos electrónicos masivos. Los expertos denominan a esta tendencia 'hiperpersonalización'. En el futuro, los ciberdelincuentes usarán cada vez más redes sociales, plataformas de empleo y mensajeros para este tipo de ataques.



¡Prueba y decide!

El mercado está repleto de útiles soluciones que proporcionarán seguridad a tus dispositivos. Algunas de las suites de seguridad más completas ofrecen un período de prueba gratuito, que te resultará muy útil para poder evaluarlas.

CINCO FALSOS MITOS

Los expertos explican que las supersticiones digitales de los usuarios aumentan el riesgo de exposición a amenazas como phishing, robo de identidad o fraude. Por ello, uno de los principales objetivos digitales debería ser romper con los siguientes cinco falsos mitos.

El estudio de 'Superstición e inseguridad: cómo se relacionan los usuarios españoles con el mundo digital', realizado por Kaspersky, revela que aún existen varias supersticiones entre los usuarios al navegar por Internet, gestionar su información personal online o utilizar dispositivos inteligentes. Esto supone un riesgo, puesto que puede llevar a las personas a mantener **comportamientos descuidados y peligrosos**, lo que las vuelve más vulnerables a amenazas como el phishing, el robo de identidad y el fraude.

Tras el análisis, los expertos de la compañía identificaron cinco mitos que impactan negativamente en la seguridad online de los españoles, y aseguran que uno de los principales objetivos digitales de los usuarios debe ser **derribar estas creencias**, para así garantizar la protección de la vida digital.

Estos son los falsos mitos identificados por Kaspersky:

1 **Los dispositivos iOS son inmunes a los ataques:** aunque estos equipos cuentan con medidas de seguridad sólidas, no son inquebrantables. Según el estudio de Kaspersky, el 22 % de los españoles cree, erróneamente, que los productos iOS no pueden ser pirateados. Esta falsa sensación de seguridad puede llevar a descuidar prácticas esenciales, como la instalación de soluciones de seguridad o la actualización regular del software. Es decir, es fundamental reconocer que todos los dispositivos requieren medidas de protección adecuadas, para así prevenir posibles amenazas.

Foto: Depositphotos.com

El malware puede infectar tu móvil sigilosamente con señales como bajo rendimiento, batería que se agota rápidamente o consumo excesivo de datos.

SOBRE CIBERSEGURIDAD

2 El modo incógnito del navegador web garantiza el anonimato online: aunque este modo impide que el historial de navegación se almacene en el dispositivo, no ofrece un anonimato completo. Sin embargo, un 38 % de los usuarios españoles cree que navegar en modo incógnito hace que su actividad en Internet sea completamente invisible, lo cual es incorrecto, ya que este sistema no protege contra el rastreo por parte de los sitios webs, proveedores de servicios de Internet o posibles atacantes. En cualquier caso, para una mayor privacidad, se recomienda siempre utilizar soluciones de seguridad integral adicionales y fiables, que se encargan de proteger los dispositivos y de identificar filtraciones de datos y contraseñas.

Foto: Depositphotos.com

Es fácil para los delincuentes crear un punto de acceso WiFi falso que parezca auténtico, imitando al de una cafetería, un aeropuerto o similar.

Foto: Depositphotos.com

Empresas rastrean tu actividad web y recopilan datos personales. El modo incógnito ayuda a reducir el seguimiento y protege tu privacidad.

3 Las redes WiFi públicas son seguras: la creencia de que es seguro utilizar redes WiFi abiertas, normalmente en cafeterías o lugares públicos, siempre que no se realicen operaciones sensibles es peligrosa. El 69 % de los encuestados españoles considera que es perfectamente seguro conectarse a redes WiFi de libre acceso en lugares públicos. Sin embargo, estas redes pueden ser fácilmente interceptadas por ciberdelincuentes, permitiendo así el robo de información personal y contraseñas de acceso. Se aconseja evitar el uso de este tipo de redes para cualquier actividad que requiera facilitar información personal y, en su lugar, se recomienda utilizar siempre conexiones seguras o redes móviles.

4 No pasa nada si accedo a enlaces que recibo por WhatsApp: según el estudio, una cuarta parte de los españoles (21 %) confía en el cifrado de extremo a extremo en servicios de mensajería como WhatsApp. Creen que esto garantiza seguridad al usar enlaces en directo. Sin embargo, este cifrado solo asegura los mensajes, no valida la seguridad de los enlaces, que podrían dirigir a sitios maliciosos. Por ello, los expertos de Kaspersky recomiendan verificar siempre los enlaces antes de pulsar en ellos, y utilizar herramientas de seguridad para mantenerse protegido en el mundo digital.

5 Al vaciar la Papelera de reciclaje del smartphone se eliminan los riesgos de seguridad: el 69 % de los usuarios cree que vaciar con regularidad la Papelera de reciclaje de sus teléfonos móviles ayuda a minimizar riesgos de ciberseguridad. Sin embargo, esta acción no tiene impacto directo en la protección contra amenazas digitales como el malware, los ataques de phishing o el robo de datos. Para protegerse, es más efectivo instalar software de seguridad, mantener las apps actualizadas y tener cuidado con los permisos que tienen las aplicaciones instaladas en el móvil.

Marc Rivero, Lead Security Researcher de Kaspersky, concluye diciendo lo siguiente: "estos mitos crean una falsa sensación de seguridad, lo que lleva a las personas a ignorar prácticas de protección adecuadas y las expone a amenazas reales que podrían haberse evitado con una mayor conciencia y educación sobre los riesgos digitales. Este año debemos derribar estos mitos, formar sobre los verdaderos riesgos y proteger nuestra privacidad en el entorno digital para aprovechar sus ventajas sin sufrir las consecuencias".

Foto: Depositphotos.com

Un antivirus actualizado reduce riesgos y protege tu privacidad.

Foto: Depositphotos.com

Los ciberdelincuentes usan la confianza en WhatsApp para difundir enlaces maliciosos, enviados por contactos conocidos, desconocidos o grupos.

KIOSKEROS

ESTO NO ES SEGURO

Phishing, fraudes, virus y estrategias inteligentes para aumentar la seguridad en teléfonos móviles y ordenadores: en este artículo encontrarás todo lo que necesitas saber en materia de ciberseguridad.

NO LE DES A 'RENOVAR'

Hay un correo electrónico circulando que parece venir del popular proveedor de servicios de pago Klarna que dice "Renovar mandato de domiciliación bancaria". Tras dirigirse personalmente al usuario, le informa de que su orden de domiciliación ha expirado recientemente. El correo electrónico menciona que es crucial tener una orden de domiciliación bancaria válida, para así poder seguir utilizando Klarna como método de pago y evitar cualquier comisión por un cargo por devoluciones de débitos. Junto al mensaje, aparece un enlace con el botón rosa 'Renovar' en la parte inferior. Y para aumentar aún más la sensación de presión, el enlace solo es válido durante 48 h. Pero ¿qué es lo que hay detrás? Un timo, ¡por supuesto! Los mensajes de este tipo pretenden persuadir a las víctimas para que hagan clic precipitadamente; al fin y al cabo, nadie quiere pagar comisiones innecesarias. Cualquiera que caiga en la trampa de este correo electrónico de phishing revelará sin saberlo sus datos bancarios y, en el peor de los casos, se convierte en víctima de una estafa. Como siempre, si encuentras mensajes de este tipo en tu bandeja de entrada, no los abras; bórralos inmediatamente. Un truco: instalarse la aplicación Klarna supone un nivel de seguridad adicional. Si realmente necesitas tomar medidas sobre un asunto, allí podrás ver el mensaje correspondiente. Este tipo de manipulación dentro de la aplicación es mucho menos probable que los correos electrónicos falsos.

MIRADAS INDISCRETAS

¿Tienes un streaming box o un SmartTV basado en Android? Entonces, no deberías dejar a un extraño a solas con él. El youtuber Cameron Gray ha descubierto que cualquier persona con acceso directo al dispositivo puede manipular la plataforma de tal forma que desbloquee todos los servicios vinculados a la cuenta de Google. Gray instaló Chrome en los dispositivos a través de métodos indirectos y se sorprendió al descubrir que el navegador podía iniciar sesión en el servicio de correo electrónico y en la nube sin necesidad de introducir una contraseña. Google quiere resolver el problema con actualizaciones.

HACKEOS POR IA

La inteligencia artificial resulta cada vez más inteligente e interesante para los piratas informáticos como herramienta. Un equipo de la Universidad de Illinois ha probado los principales modelos de IA respecto a las vulnerabilidades de seguridad conocidas, pero que aún no se han solucionado. El resultado: ChatGPT 4 encontró varias formas efectivas de explotar esas vulnerabilidades en el 87 % de los casos, mientras que los otros modelos solo presentaron un éxito limitado.

VIRUS EN YOUTUBE: VÍDEOS PELIGROSOS

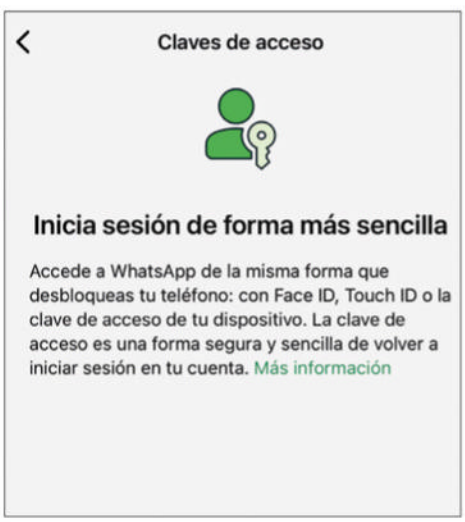
YouTube es una plataforma de entretenimiento fantástica, pero por desgracia algunos vídeos también conllevan determiandos riesgos ocultos. Al parecer, desde hace poco tiempo, los delincuentes han intentado propagar programas maliciosos a través de esta plataforma. Un equipo de investigadores de la empresa de seguridad Proofprint ha descubierto toda una serie de vídeos que enseñan cómo desbloquear ilegalmente videojuegos u otro tipo de software. Los 'cracks' necesarios (y contaminados) para ello se enlazan en los comentarios de texto correspondientes y esos archivos contienen virus. En realidad no se trata de algo nuevo, pero los hackers están empleando mucho más este enfoque últimamente.

RUSIA OBSTACULIZA LA AVIACIÓN

La guerra entre Rusia y Ucrania está repercutiendo en el tráfico aéreo civil: cada vez hay más informes sobre interrupciones en la recepción GPS. Los aviones utilizan esta señal de satélite para determinar correctamente su posición. Los servicios militares y de inteligencia occidentales han identificado el llamado Baltic Jammer como la razón de dichas interrupciones. Se trata de un transmisor de interferencias que, al parecer, se encuentra en la región rusa de Kaliningrado. Por ello, el tráfico aéreo en Polonia, los países bálticos, el sur de Suecia y Alemania se ve especialmente afectado. Pero no te preocupes: los aviones también pueden utilizar un tipo de tecnología de navegación alternativa si se interrumpe el GPS, por lo que no hay peligro.

WHATSAPP: AHORA TAMBIÉN HAY PASSKEYS EN APPLE

Las llamadas passkeys (claves de acceso) son cada vez más populares. Permiten iniciar sesión en aplicaciones mediante reconocimiento facial o huellas dactilares, sin necesidad de establecer una contraseña clásica en segundo plano. En su lugar, utilizan un procedimiento criptográfico. Desde hace algún tiempo, WhatsApp para Android también ofrece la opción de protección mediante una passkey. Y, ahora, esta función también está disponible para iOS. Si quieres proteger tu cuenta de WhatsApp con una passkey, abre la app y toca en ***Configuración***, ***Cuenta*** y ***Claves de acceso***. A continuación, especifica qué tipo de autorización quieres utilizar.



CHATBOT CONTRA EL FRAUDE

El especialista en seguridad Bitdefender está expandiendo su chatbot gratuito Scamio y ha incluido en él una nueva integración con WhatsApp. De esta forma, ahora puedes enviar fácilmente al contacto de Scamio en WhatsApp cualquier mensaje sospechoso, foto o archivo PDF para recibir directamente ahí una evaluación sobre si supone una amenaza real o no. Si quieres probarlo en este mismo momento, escanea el código QR que se ve arriba aquí. Para lograrlo, tendrás que registrarse, pero el servicio en sí no cuesta nada.

KIOSKEROS

ALTERNATIVAS A LOS SERVICIOS ESTADOUNIDENSES

TU BOLSILLO Y TUS

Donald Trump lanza una guerra comercial contra el mundo. ¿Qué significa esto para nuestros datos? ¿Siguen estando seguros? ¿Y qué alternativas europeas existen?

La mayoría de los usuarios utiliza más de un servicio estadounidense. Ya sea Netflix, Amazon, Google o OneDrive: todos estos servicios digitales provienen de Estados Unidos. Hasta ahora, esto no había supuesto un problema significativo para los usuarios en Europa. Sin embargo, con la segunda presidencia de Donald Trump, el panorama ha cambiado. **Trump ha anunciado aranceles** devastadores a nivel mundial. La caída drástica de las cotizaciones bursátiles y el aumento de los precios al consumidor amenazan con repercutir también negativamente, a largo plazo, a los consumidores europeos.

¿Y por qué todo esto? Según Trump, la balanza comercial con Europa y el resto del mundo es desfavorable para EE. UU. Muchos expertos no están de acuerdo. Especialmente en los servicios digitales mencionados, el dominio es abrumadoramente a favor de Estados Unidos. Pero Trump podría utilizar esto como palanca contra Europa, **encareciendo artificialmente el precio** de estos servicios. Por suerte, existen buenas alternativas europeas.

Cuentas de correo electrónico

Las cuentas de correo electrónico contienen nuestra comunicación privada, incluidas conversaciones con empresas y organizaciones, y por lo tanto, una gran cantidad de información personal. Alternativas europeas:

- GMX (Alemania)
- Posteo (Alemania)
- Proton Mail (Suiza)
- Mailbox.org (Alemania)

Navegadores web

Tu navegador guarda qué páginas abres, cuándo y durante cuánto tiempo navegas, qué haces en los sitios web, qué buscas y mucho más. Estos datos se utilizan para averiguar muchas cosas sobre ti. Alternativas europeas:

- Vivaldi (Noruega)
- Mullvad Browser (Suecia)

Programas de correo electrónico

En los programas de correo, se almacenan mensajes de todas las cuentas, a menudo acumulados durante años. Estos pueden incluir facturas, credenciales de acceso, fotos, solicitudes de empleo y más. Alternativas en Europa:

- emClient (República Checa)
- The Bat! (Moldavia)

Servicios de pago online

Los proveedores de servicios de pago son capaces de ver qué compras, cuándo y dónde lo haces, y pueden crear un perfil detallado sobre ti. Además, es posible que las tarifas aumenten para los europeos o que te cobren una tarifa básica. Algunas alternativas europeas:

- Bizum (España)
- Klarna (Suecia)

Ofimática

Microsoft Office, según la propia compañía, guarda los documentos en servidores europeos. Sin embargo, quien no quiera depender de esto siempre puede optar por alternativas europeas:

- Ashampoo Office (Alemania)
- Softmaker Office (Alemania)
- LibreOffice (Alemania)

Redes sociales (profesionales)

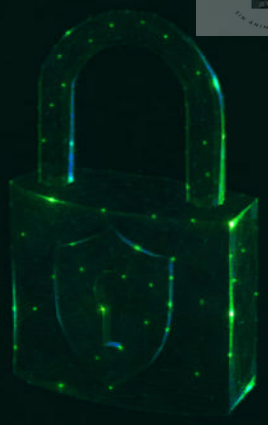
Los contactos y la comunicación profesional pueden resultar muy interesantes en determinados trabajos, pero ahí se maneja información sensible. Los proveedores de estas redes podrían ser obligados por el gobierno de EE. UU. a permitir el acceso a las autoridades estadounidenses.
Una alternativa europea:

- Xing (Alemania)

¿QUÉ PASA CON LOS ANTIVIRUS?

En Estados Unidos, también se encuentran algunas empresas de seguridad como McAfee y Gen Digital con su marca subsidiaria Norton. ¿Es esto por sí solo un buen motivo para cambiar a proveedores europeos como G-Data (Alemania) o Bitdefender (Rumanía)? No necesariamente, ya que en exhaustivas pruebas de laboratorio pudimos comprobar la protección de primera de nuestro ganador del test, Norton 360 Advanced. Esto debería ser un factor más decisivo para garantizar la máxima seguridad que cualquier recelo infundado hasta ahora.

DATOS A SALVO



Almacenamiento cloud

Los archivos importantes que no quieres perder y que no deben caer en manos malintencionadas también se pueden almacenar online. Existen estas alternativas:

- Proton Drive (Suiza)
- koofr (Eslovenia)
- Filen (Alemania)
- Cozy (Francia)

Mensajería

A través de aplicaciones de mensajería como WhatsApp, gran parte de la comunicación con amigos y familiares tiene lugar de manera cifrada. Sin embargo, existe el riesgo de que los usuarios europeos puedan ser excluidos o deban pagar por el servicio. Algunas alternativas son:

- Threema (Suiza)
- Olvid (Francia)

Gestores de contraseñas

Los sistemas de almacenamiento de los gestores de contraseñas se encuentran cifrados. Si se pierde el acceso, se perdería también la clave para todos los servicios online del usuario y sería necesario restablecer las contraseñas una por una. Alternativas en Europa:

- Passwort Depot (Alemania)
- Proton Pass (Suiza)

Almacenamiento de fotos

En Google Fotos, muchas personas almacenan todas sus imágenes. Aunque no se desean perder esos recuerdos, existe el riesgo de que datos sensibles de reconocimiento facial puedan caer en manos de hackers o gobiernos. Alternativas interesantes:

- Jottacloud (Noruega)
- pCloud (Suiza)
- Immich (código abierto)

Compras online

Si en EE. UU. se cobran aranceles al importar productos, es probable que Europa aplique aranceles de represalia. Si quieres apoyar al comercio europeo, puedes optar por alternativas europeas:

- PcComponentes (España)
- Zalando (Alemania)
- MediaMarkt (Alemania)
- Ikea (Suecia)
- H&M (Suecia)

Motores de búsqueda

Con el historial de búsqueda se puede crear un perfil transparente de ti, con todas las páginas que has visitado y todos los términos que has consultado. Aquí tienes algunas alternativas:

- Qwant (Francia)
- Search.ch (Suiza)

Apps de navegación GPS

Los navegadores GPS te ayudan a encontrar el camino correcto. Sin embargo, el proveedor también puede saber dónde estás, cuándo sueles transitar por ciertos lugares y mucho más. Algunas alternativas europeas:

- Komoot (Alemania)
- TomTom (Países Bajos)
- HERE WeGo (Países Bajos)

Películas y series en streaming

Qué películas y series ves no debería ser realmente interesante para nadie. Sin embargo, este tipo de plataformas podrían volverse más caras fuera de EE. UU. Algunas alternativas europeas:

- Filmin (España)
- Mubi (Reino Unido)

Inteligencia Artificial

Las IA se utilizan tanto en el ámbito profesional como personal para muchos fines, como escribir textos, traducir, programar y mucho más. A través de estas herramientas, terceros pueden conocer mucho sobre ti.
Una alternativa europea:

- Le Chat (Francia)

Streaming de música

En el caso concreto de la música, la preocupación suele estar más enfocada en los precios y el acceso que en el interés por espiar tus hábitos de escucha. Algunas alternativas europeas son:

- SoundCloud (Alemania)
- Spotify (Suecia)
- Deezer (Francia)

Redes sociales (privadas)

Con la información de Facebook, Instagram, Snapchat y otras redes sociales, se puede descubrir mucho sobre ti como persona privada. Incluso fotos y vídeos podrían ser utilizados para el reconocimiento facial. Pero ¿qué alternativas interesantes de Europa hay?

- ... ino existen!

Videoconferencia

Los videochats y las videoconferencias deberían mantenerse sin oyentes secretos. Con la IA, sería fácil grabar todo en segundo plano o generar transcripciones. Algunas alternativas europeas:

- Ionos (Alemania)
- Jitsi (Francia)

CONTRA EL MALWARE Y EL SPAM

LLEGAN LOS DNS DE LA

Europa busca su independencia tecnológica y, recientemente, ha dado un paso más al presentar los DNS europeos. Este sistema quieren romper la dependencia de las compañías estadounidenses y es más privado y seguro.

Adiós Google, adiós Cloudflare, hasta nunca DNS de las operadoras! Ha llegado el momento de cambiar a **DNS4EU**, el nuevo Sistema de Nombres de Dominio creado por la Unión Europea para mantener los datos de navegación web dentro de Europa y, al mismo tiempo, frenar el malware, el spam, y el contenido inapropiado para los menores.

En términos generales, DNS es el sistema que traduce las direcciones web, como **www.google.es**, en la dirección física del servidor donde se aloja esa página, es decir, su dirección IP. Algo así como **243.23.232.114**. Esta 'traducción' se realiza utilizando unos servidores DNS y, aunque la inmensa mayoría de los usuarios utiliza las direcciones DNS de su operadora, muchos cambian a las DNS de Google, que suelen ser más rápidas, o las de Cloudflare, que ofrecen mayor privacidad. Sin embargo, hay muchas más...

Foto: Depositphotos.com

La UE impulsa sus propios DNS para evitar que terceros conozcan dónde navegas, protegiendo la privacidad de los usuarios europeos en Internet.

Así son los DNS de la UE

El problema de los servidores DNS es que, al encargarse de traducir los nombre de dominio en direcciones IP para acceder a páginas web o servicios de Internet, pueden **registrar todas las páginas que visita** cada usuario. Esta es una información muy valiosa, y está en manos de compañías estadounidenses como Google y Cloudflare, que además no cumplen las estrictas **normas de privacidad de la Unión Europea**. Por esta razón, la Comisión Europea encargó a la Agencia de Ciberseguridad de la Unión Europea (ENISA), la creación de servidores DNS más privados y seguros, para que puedan utilizarlos los usuarios de la UE. Este sistema se llama DNS4EU, y ya está aquí.

Según explica la web de DNS4EU (**www.joindns4.eu**), estas DNS cumplen el Reglamento General de Protección de Datos de la UE (GDPR), así que son más privados y seguros que los norteamericanos. Y, según el servidor que elijas, protegen contra el malware, el spam o el contenido para adultos. Para ello, en la configuración de In-

Foto: Xxxxxxxxxxx

KIOSKEROS

UE

ternet de tu dispositivo, simplemente tienes que eliminar el DNS que tengas establecido y añadir el que más te convenga de DNS4EU. Hazlo según esto:

- **Sistema DNS sin filtros (86.54.11.100): *IPv6 2a13:1001::86:54:11:100*** No aplica ningún tipo de bloqueo ni filtrado. Es ideal para usuarios que ya tienen medidas de seguridad propias y prefieren una navegación rápida, sin restricciones ni modificaciones.
- **Sistema de protección contra webs malignas y fraudulentas (86.54.11.1): *IPv6 2a13:1001::86:54:11:1*** Se encarga de filtra sitios peligrosos o fraudulentos, como los que contienen malware o intentos de robo de datos (phishing), pero permite el acceso a todo el contenido general, incluyendo anuncios.
- **Sistema de protección infantil (86.54.11.12): IPv6 2a13:1001::86:54:11:12** Se encarga de filtrar sitios con contenido inapropiado para niños, pero no bloquea la publicidad. Resulta útil en entornos familiares o escolares.
- **Protección infantil, spam y publicidad (86.54.11.11): IPv6 2a13:1001::86:54:11:11** Bloquea el acceso a sitios con contenido inapropiado para menores (como violencia, pornografía o drogas) y también elimina los anuncios de páginas web y aplicaciones. Es recomendable solo en dispositivos privados. En cualquier caso, hay que tener en cuenta que algunos sitios o apps pueden no funcionar bien si detectan bloqueadores de anuncios.
- **Protección contra spam y publicidad (86.54.11.13): IPv6 2a13:1001::86:54:11:13** Oculta los anuncios en webs y aplicaciones, además de ofrecer protección contra sitios maliciosos. Como en el resto de los casos, algunos sitios pueden verse afectados si emplean sistemas que bloquean el acceso cuando detectan bloqueadores de anuncios.

Foto: Depositphotos.com

Los nuevos DNS europeos integran filtros que bloquean webs maliciosas o fraudulentas, ofreciendo de esta manera una navegación más segura sin depender de proveedores tecnológicos privados o extranjeros.

Ten en cuenta que estos sistemas de DNS europeos aún están en fase beta, así que puede producir algún fallo o ralentización. En cualquier caso, si quieres aumentar la privacidad y evitar que Google, Cloudflare o cualquier otra operadora sepan las webs que visitas, el sistema DNS4EU anonimiza el acceso, y además protege del **malware, el spam, la publicidad** excesiva y el contenido para adultos, según elijas. Cada opción está pensada para diferentes tipos de usuarios y, por ello, antes de aplicar una configuración concreta, conviene probarla en tus dispositivos habituales para de esta forma asegurarte de que todo funciona correctamente. ■

ASÍ DE FÁCIL PUEDEN LOS HACKERS DESCIFRAR TUS CONTRASEÑAS

Las contraseñas dan acceso a cosas importantes como cuentas de correo electrónico y servicios de pago, pero averiguarlas puede ser muy sencillo.

¿Crees que tu contraseña es segura? La realidad es bastante preocupante: la mayor parte de las contraseñas que hasta hace unos años se consideraban seguras, ahora pueden descifrarse en cuestión de horas o incluso en segundos. **Las reglas básicas de siempre ya no son válidas**, y las contraseñas seguras ahora son tan largas que nadie puede recordarlas. Computer Hoy te explica los métodos más comunes que usan los hackers para descifrar las contraseñas, y cómo puedes protegerte frente a estos.

Crackeadores profesionales

Los hackers están especializados en descifrar contraseñas y, por lo general, lo logran a base del método de ensayo y error. Si, por ejemplo, consiguen hacerse con una base de datos de un proveedor, las contraseñas que este almacena se guardan de forma cifrada, Pero la función de cifrado es conocida, y lo que hacen es introducir en ella y de forma masiva posibles contraseñas comparando los resultados. Es solamente una cuestión de tiempo el que encuentren la clave correcta, y el tiempo que pase hasta conseguirla vendrá determinado por los siguientes factores:

- **Complejidad de la contraseña:** cuanto más sencilla sea la clave, más rápidamente podrá descifrarse. Las contraseñas más populares o las típicas variaciones de las mismas, por ejemplo sustituyendo letras por números, es lo primero que prueban los ciberdelincuentes. En estos casos concretos, tan solo necesitarán unos segundos. Seguidamente, llega la fase de probar de manera sistemática todas las combinaciones existentes posibles. En primer lugar, los hackers empiezan con contraseñas cortas y van avanzando lentamente hasta llegar a otras que sean más largas.
- **Cifrado:** el método de cifrado que se haya usado influye mucho en el tiempo que durará el proceso. Ignas Valancius, responsable de Ingeniería de NordPass, nos explica que una tarjeta gráfica RTX 4080 de Nvidia aborda una cantidad diferente de ensayos por segundo, todo ello en función del algoritmo de cifrado que se haya utilizado previamente:
  - **Bcrypt:** 131.200
  - **SHA2-512:** 4.460.200
  - **SHA2-256:** 13.075.800
  - **SHA1:** 30.397.900

¿CUÁNTO TIEMPO SE TARDA EN DESCIFRAR UNA CONTRASEÑA?

En la siguiente tabla, hemos indicado los tiempos aproximados que se tarda en descifrar contraseñas de distintos tipos con un PC de tipo medio. En el sitio web **nordpass.com/secure-password**, puedes calcular el tiempo que se tardaría en descifrar tu contraseña.

Tipo de contraseña	Tiempo de descifrado
Palabras	1 segundo
8 caracteres incluyendo un número	1 hora
8 caracteres, incluidos números, mayúsculas y caracteres especiales	3 horas
10 caracteres, incluidos números, mayúsculas y caracteres especiales	12 días
12 caracteres, incluidos números, mayúsculas y caracteres especiales	3 años
16 caracteres, incluidos números, mayúsculas y caracteres especiales	Más de 1.000 años

- **MD5:** 98.262.800
- **MD4:** 175.800.000.000

Estas cifras revelan, por ejemplo, que el algoritmo de cifrado Bcrypt es más de un millón de veces mejor que el denominado MD4.

- **Potencia de procesamiento:** las CPU o los procesadores de las tarjetas gráficas son los encargados de realizar el trabajo de descifrado. Cuanto más rápido y potente sea el procesador y más núcleos tenga, más cálculos y ensayos por segundo podrá llegar a hacer.

En el cuadro de la parte izquierda de la página anterior, puedes ver los tipos de contraseñas más comunes y el tiempo que se tarda en descifrarlas. Según nos explica Valancius, algunos hackers usan también **PC equipados con varias tarjetas gráficas**, de igual forma que se hace en el minado de criptomonedas (ver cuadro superior derecho). De esta forma, se aumenta substancialmente la velocidad.

¿Cuándo atacan los hackers?

Los ciberdelincuentes también piensan en términos de rentabilidad: cuanto mayor sea el posible botín y menor sea el esfuerzo necesario para lograrlo, más probable será que se ejecute un ataque. Lo que hacen es simplemente probar las contraseñas 'sustraídas' en otros sitios. Si los titulares de las cuentas usan las mismas contraseñas o similares en otras plataformas, es probable que los delincuentes puedan acceder a datos de pago o información privada. Acostumbran a realizar ataques muy específicos contra **personajes famosos o personas importantes**, ya que en estos casos suele haber, por lo general, más de dónde sacar.

Existen diferentes motivos por los que una persona puede ser un objetivo interesante desde el punto de vista del ciberdelincuente, y esto no siempre se encuentra relacionado con que la víctima sea un personaje famoso. Por ejemplo, pueden escoger como objetivo a los empleados de grandes empresas. También se producen constantemente ataques de fuerza bruta a proveedores de servicios de correo electrónico, en los que los atacantes intentan conseguir acceso a las cuentas de forma aleatoria. Existe, por tanto, un peligro real para cualquier usuario de Internet.

Cómo protegerse

Como ya se ha comentado anteriormente, la rapidez con la que puede descifrarse una contraseña depende también del método de cifrado usado por el sitio web o la cuenta en cuestión. Puedes (y deberías) informarte sobre este aspecto, aunque no puedas hacer nada para modificarlo o cambiarlo. Es por ello que es tan importante usar siempre una contraseña segura. Las reglas básicas tradicionales como usar 'ocho caracteres, un carácter especial y una mayúscula', ya no sirven. Una contraseña que aplique este sistema podría descifrarse en 3 h como máximo. A partir de doce caracteres, usando caracteres especiales, números y mayúsculas, se consigue una contraseña relativamente segura, que puede necesitar meses para descifrarse. Pero lo mejor es **si contiene 16 caracteres o más**. En ese caso, los hackers necesitarán miles de años para descifrar la contraseña. Una clave de esta longitud debería seguir siendo segura si tenemos en cuenta que la potencia de cálculo de las tarjetas gráficas se duplica cada dos años, lo que permitiría reducir a la mitad el tiempo necesario para descifrarla. Obviamente nadie puede memorizar contraseñas tan monstruosamente largas, y por ello existen los gestores de contraseñas (ver apartado superior). ■

EL HARDWARE QUE SE UTILIZA PARA DESCIFRAR CONTRASEÑAS

Los hackers individuales utilizan normalmente ordenadores estándar para descifrar contraseñas. Pero los grupos de hackers más grandes o los ciberdelincuentes especializados en este tema disponen de ordenadores especiales que hacen uso de varias tarjetas gráficas de alto rendimiento. Las tarjetas gráficas de este tipo trabajan en paralelo e incrementan la velocidad a la que se descifran las contraseñas. Por poner un ejemplo, si un PC normal necesita un mes de trabajo para descifrar una contraseña, uno equipado con seis tarjetas gráficas, podría tardar únicamente cinco días. Los grupos de ciberdelincuentes usan además centros de datos alquilados o botnets, lo que se traduce es que tan solo tardarán unas horas o minutos.

Un PC equipado con varias tarjetas gráficas reducirá significativamente el tiempo necesario para descifrar las contraseñas.

UN GESTOR DE CONTRASEÑAS PARA MANTENERSE PROTEGIDO

Junto con la autenticación de dos factores o 2FA, los gestores de contraseñas son una forma eficaz de protegerse. Mientras que la autenticación de dos factores en muchas ocasiones no está activada y por ello puede ser burlada, los gestores de contraseñas permiten usar claves particularmente largas y seguras, sin que los usuarios tengan que memorizar extensas cadenas de caracteres. Incluso los mejores hackers con el mejor equipo pueden estamparse de bruces contra combinaciones tan seguras. Además, con esto se consigue otra ventaja, y es que los gestores de contraseñas facilitan el inicio de sesión en sitios web, al hacerlo por ti de forma automática. Esto te permitirá no quedarte bloqueado en la función 'olvidaste tu contraseña' y tener que restablecer tu contraseña constantemente. Por otro lado, los gestores de contraseñas también te alertan si las cuentas y contraseñas que hayas introducido están circulando por la Darknet. En el número 675 de Computer Hoy, en nuestro especial de seguridad, probamos 6 gestores de contraseñas, y el ganador de la comparativa fue NordPass Premium de Nord Security. Recuerda que un buen gestor de contraseñas tiene un coste de tan solo unos pocos euros al mes y las versiones más sencillas, sin prestaciones adicionales, suelen ser gratuitas.

KIOSKEROS

VULNERABILIDAD DE SEGURIDAD EN LOS ROUTERS

¿SUPONE UN PELIGRO PARA LAS VPN?

Según un estudio sobre seguridad, la vulnerabilidad conocida como TunnelVision, que cuenta ya con más de 22 años de antigüedad, podría paralizar los servicios VPN. Pero ¿podría esto ocurrir realmente?

La empresa de seguridad estadounidense Leviathan Security es quien ha publicado la información que ha caído como una bomba: en un estudio realizado se revela que un atacante podría, manteniendo la apariencia de una conexión segura, **interceptar el tráfico de datos** de cualquier usuario de un servicio VPN. La artimaña se realiza mediante la manipulación del router, direccionando el tráfico a un canal no cifrado fuera de la VPN. La culpable de que esto sea posible es una función poco conocida del protocolo DHCP denominada 'option 121'. No se trata en absoluto de un problema nuevo, ya que por primera vez se informó de ello en 2002 y, según Leviathan Security, podría provocar "una filtración total de las VPN". El asunto ha generado una gran controversia y los expertos coinciden en que, para la mayor parte de los ordenadores, no existe por el momento una solución completa que solvente el problema. La noticia provocó en Internet un enorme revuelo e intranquilidad, puesto que son muchos los usuarios que confían en la seguridad de las VPN.

¿Qué peligro representa?

Entonces, ¿podrían estar en entredicho los servicios de ocultación VPN debido al descubrimiento de la vulnerabilidad TunnelVision? Por suerte, la cosa no es tan sencilla. Para empezar, la mayor parte del tráfico web está cifrado a través de HTTPS, incluso sin contar con una VPN. Es por este motivo que, si el tráfico de datos terminara redirigiéndose a un canal fuera del túnel VPN, el atacante podría ver alguna información de tipo metadato, pero nunca el tráfico de datos en un formato legible. Además, cuando se accede a un sitio HTTP (sin S), lo que ya de por sí es algo extraño, la responsabilidad recae en el propio usuario, puesto que los navegadores como Chrome o Firefox advierten de que se está visitando un sitio inseguro, y estos únicamente permiten el acceso **tras la previa confirmación** por parte del usuario. Leviathan así lo admite también: "Aunque el tráfico HTTPS quedara expuesto, seguiría siendo imposible ver el contenido cifrado del paquete", declara la empresa. "Sin embargo, sí sería posible conocer el destino y el protocolo del paquete. Por regla general, esta información reside en la carga útil del protocolo VPN y se encuentra cifrada". Además, un atacante tendría primero que apañárselas para manipular el router. Y es más que cuestionable que esto pudiera llevarse a cabo fácilmente en el caso de un proveedor de Internet o de telefonía móvil. Estos dispositivos suelen encontrarse bajo la supervisión absoluta de un administrador de sistemas. Sin embargo, donde sí podría representar un problema y un riesgo sería, por ejemplo, en los puntos de acceso de hoteles o restaurantes.

La opinión de los proveedores de VPN

Los proveedores de VPN más importantes respondieron al estudio de Leviathan casi de inmediato aclarando su posición. El más contundente fue ExpressVPN: "Si te encuentras en casa y nadie ha accedido a tu router, estás protegido. Si te conectas a Internet a través de la red móvil y no a través de la red WiFi de alguien ajeno, estás protegido. Si la red WiFi a la que te conectas no está controlada por alguien malintencionado, estás protegido. Si te conectas a Internet a través de tu portátil y tienes activada la función Kill Switch, estás protegido, etc. En la práctica, deben **confluir muchos factores al mismo tiempo** para que este problema pudiera suponer un riesgo", aclara ExpressVPN en una publicación de su página web. NordVPN también opina de forma parecida. Un portavoz de la empresa nos comentó: "Ninguna de nuestras aplicaciones puede filtrar el flujo de datos si están activadas en el menú de configuración las funciones 'Permanecer invisible en una red local' y 'Kill Switch'. Un ataque a través de un canal lateral podría provocar la pérdida

de la conexión a Internet, pero no se permitiría la filtración de datos". Teóricamente, según NordVPN, debería cumplirse toda una serie de condiciones para que un ataque tuviera éxito; no bastaría con que alguien consiguiera acceder a la red a la que está conectado el objetivo. Mediante el uso de procedimientos de eliminación, como por ejemplo bloqueando determinadas direcciones IP, el atacante podría, en el mejor de los casos, suponer que la persona que busca es la que accede a una determinada página en un momento dado, pero incluso en ese caso, "los atacantes **no podrían conocer el contenido real** al que accede la persona objetivo".

Activación de Kill Switch

Si se quiere descartar cualquier posible riesgo, lo mejor sería activar **la función Kill Switch de la VPN en Windows, macOS o Linux**, si es que no está ya activada de forma predeterminada en el sistema, que es precisamente la medida que recomiendan prácticamente todos los proveedores de servicios VPN. Más problemático sería el proceder en iOS, puesto que la arquitectura del sistema de Apple no permite configurar por completo una función Kill Switch. En cualquier caso, habrá que ver cómo se solucionará esta brecha de seguridad en un iPhone y iPad. Por lo menos, Mullvad VPN dice que está trabajando en una solución para estos dispositivos iOS. Por su parte, los usuarios de Android no tienen de qué preocuparse a este respecto, ya que el sistema operativo móvil de Google simplemente ignora la función Option 121.

¿QUÉ ES **KILL SWITCH**?

Una VPN protege todo el tráfico de datos y oculta la dirección IP. Si de forma accidental se interrumpe la conexión VPN, el anonimato y la ocultación también se interrumpe. Para evitar que tu propia dirección IP quede expuesta y vinculada al tráfico de datos, los proveedores de VPN integran un interruptor o conmutador de emergencia en sus aplicaciones, el 'Kill Switch'. Este sistema lo que hace es desconectar la conexión a Internet, sin más preámbulos, hasta que se restablezca de forma adecuada la conexión con el servidor VPN. A pesar de lo importante de este mecanismo, el sistema Kill Switch de la VPN no viene activo de forma predeterminada en la configuración de la mayoría de proveedores de servicios de VPN. Debes buscar la función en los ajustes de tu aplicación de ocultación, y activarla entonces. Los proveedores de servicios VPN a veces también denominan la función Kill Switch como 'cortafuegos' o 'bloqueo de acceso a Internet'. Hay algunos proveedores, como es el caso de NordVPN (véase la imagen de la izquierda), que ofrecen esta función con diferentes niveles de alcance o aplicación. En cualquier caso, estas son las variantes más comunes:

- **Kill Switch estándar:** esta función lo que hace es cortar la conexión a Internet solo si se detecta un problema. Esta es la variante que ofrece el mejor nivel de compromiso entre seguridad y comodidad, y resulta más que suficiente para dar respuesta a la vulnerabilidad TunnelVision.
- **Kill Switch fuerte:** aquí la función actúa en caso de problemas; el acceso a Internet solo es viable a través de una conexión VPN activa. El servicio debe ejecutarse siempre en segundo plano, incluso si no se desea utilizar la VPN.
- **Kill switch a nivel de aplicaciones:** esta última variante de Kill Switch bloquea únicamente las aplicaciones individuales que se hayan definido para su detención, en caso de que falle la conexión VPN.

> "Para proteger la privacidad del usuario, es conveniente tener la función Kill Switch activada."
>
> **Thomas Glenk**
> Redactor

Los deepfakes son vídeos generados por ordenador de personas reales. Su uso está muy extendido en la industria del cine, para hacer que los actores parezcan más jóvenes en las películas o bien para dar vida en la pantalla a estrellas ya fallecidas. Sin embargo, puesto que las posibilidades que nos ofrece la IA están ahora mismo al alcance de cualquiera, los delincuentes pueden usar estos deepfakes para llevar a cabo las estafas más sofisticadas. En los últimos tres años, los intentos de estafa mediante el uso de tecnologías de inteligencia artificial generativa (genAI), y específicamente el uso de deepfake, **han aumentado un 2.137 %**, según datos de Signicat. Los estafadores están ganando terreno y los avances tecnológicos actuales les facilitan cada vez más su tarea delictiva. Te explicamos ahora, en estas páginas, a qué peligros nos enfrentamos con esta tecnología y cómo podemos protegernos.

Tan solo basta una foto

Hasta no hace mucho, para crear un deepfake era preciso contar con fotos de la persona en cuestión, tomadas desde diferentes ángulos y en todas las perspectivas posibles. La creación un vídeo creíble suponía un trabajo concienzudo de varias horas, pero hoy en día **basta con disponer de una foto** que tenga una calidad medianamente buena, para así crear una copia perfecta de un sujeto en cuestión de segundos. Además, para lograr resultados aparentes, los delincuentes ni siquiera necesitan tener conocimientos avanzados de informática o habilidades especiales, basta con pulsar un botón en una herramienta de IA (las fotos que necesitan las pueden encontrar fácilmente en las redes sociales). En Computer Hoy, nos hemos puesto en marcha: hemos probado a crear un deepfake y hacer un experimento con la ayuda de la empresa Sumsub, especializada en la verificación de identidades (ver recuadro inferior derecho). ¡Los resultados son inquietantes!

Posibilidades infinitas para perpetrar el fraude

Una vez que un delincuente ha creado un deepfake de calidad, existen multitud de posibilidades para actuar. Por ejemplo, podrían hacerse pasar por directivos de la empresa para solicitar un pago u obtener información sensible. Pero también cabe la posibilidad de centrarse en particulares. ¿Quién podría pensar que se trata de un fraude si es tu propio hijo el que te hace una videollamada en la que te pide dinero, todo ello respaldado por una historia perfectamente creíble? Otro supuesto podría ser que te mostraran fotos desnudas de tu hija y los estafadores amenazaran con su difusión en el trabajo o colegio. Lo importante es que da igual si las fotos son reales o generadas mediante la IA, porque el resultado y el daño causado es el mismo.

> Las empresas deberían usar IA y medidas de protección en varios niveles para protegerse a ellas mismas y a sus clientes de los deepfakes.

Pavel Goldman-Kalaydin
Director de inteligencia artificial y aprendizaje automático en Sumsub

Este es otro caso que ya ha sucedido: los delincuentes solicitan un préstamo en nombre de sus víctimas. Para ello, usan fotos y copias de documentos de identidad obtenidos en la darknet para crear un deepfake. Con este método, es posible hacer una videollamada que supere los controles de identidad online más profesionales. Estas tácticas y trucos ya los están usando los delincuentes para conseguir sumas importantes de dinero.

Reconocer un deepfake no es una tarea sencilla

Aunque muchos deepfakes presentan todavía algunos defectos y problemas como breves distorsiones de la imagen, contornos que son demasiado perfectos o movimientos de los labios que no se ajustan con precisión al audio del vídeo, esto es algo que no ocurre en todos. Los deepfakes bien hechos **no se detectan tan fácilmente a simple vista**. ¡Haz una prueba tú mismo! Los expertos del sitio web **www.sumsub.com/deepfakes**, ofrecen un juego en el que puedes poner a prueba tu capacidad para detectar lo que es y no es un deepfake. La tecnología de la IA y las

EL PELIGRO DE LOS DEEPFAKES

Con la ayuda de la IA y una única foto, los estafadores pueden crear en un santiamén una copia perfecta de ti y engañar a otras personas para causarles un perjuicio económico. ¡Protégete!

herramientas de deepfake están mejorando continuamente y, por ello, no se puede dejar en manos de individuos o empleados la tarea de detectar lo que es, o no es, una falsificación.

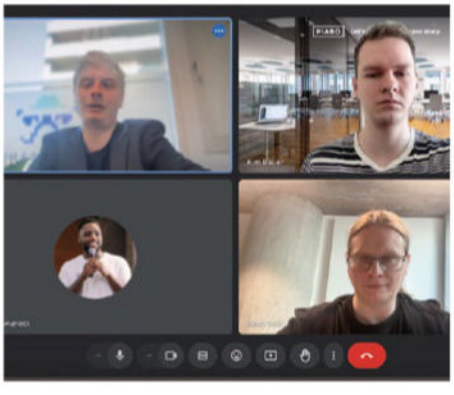
Este trabajo debe delegarse en una IA avanzada, que sea **capaz de analizar la imagen** de las videollamadas automáticamente y mostrar una advertencia cuando detecte que se trata de un deepfake. Pavel Goldman-Kalaydin, que es director de Inteligencia Artificial y Aprendizaje Automático en Sumsub, recomienda que las empresas hagan uso de la IA y apliquen medidas de protección en varios niveles para protegerse ellas mismas y a sus clientes. Aunque es verdad que ya hay personas trabajando en el área de la detección de deepfakes, no existen herramientas fiables que puedan advertir en directo, en una videollamada, que se trata de un deepfake. Y es ahí donde proveedores importantes, como son WhatsApp, Microsoft y compañía, deberían desarrollar con urgencia este tipo de soluciones, dado que el fraude se comete con sus servicios y aplicaciones, y amenaza a sus propios usuarios.

La política no puede hacer nada

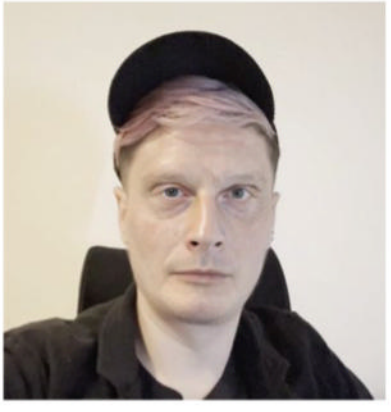
En otras ocasiones, se han solicitado **leyes que protejan a las personas e instituciones** de los deepfakes, o bien que se prohíba el uso de esta clase de aplicaciones. Sin embargo, este tipo de leyes no puede ofrecer mucho, ya que las estafas y los chantajes ya son de por sí punibles. Pero ¿quién se preocupa en la Darknet porque una herramienta esté prohibida o no? Pues, nadie. Si se produce un ataque o estafa mediante el uso de deepfakes y se detienen a los responsables, el crimen cometido ya implica cargos suficientes para su castigo. Desafortunadamente, estos delincuentes suelen encontrarse fuera del país y **ocultan sus identidades en Internet**. Lo único que puedes hacer, como particular, para poder protegerte frente a los deepfakes mientras se desarrollan soluciones que los detecten de manera fiable, es tener el máximo cuidado con las fotos y vídeos propios que publicas en Internet. No los compartas de manera pública. Hazlo solo con amigos y conocidos en los que confíes. Siguiendo esta recomendación, podrás evitar que los delincuentes encuentren material propicio que les sirva para crear deepfakes con tu rostro. Además, podrías acordar el uso de una palabra clave con tu familia y amigos cercanos para asegurarte de que la persona al otro lado de la pantalla es realmente quien dice ser. Si no has acordado ninguna y te entraran las dudas, pregunta algo que solo la persona real podría responder para estar completamente seguro.

EXPERIMENTO: ASÍ DE RÁPIDO SE CREA UN DEEPFAKE

Para comprobar la rapidez con la que es posible crear un deepfake y los inquietantemente buenos que pueden llegar a ser los resultados, hemos llevado a cabo un experimento en directo con ayuda de la empresa Sumsub en una videollamada. El experto en seguridad Pavel Goldman-Kalaydin ha copiado el rostro de Andy Voß (en pequeño abajo a la derecha) partiendo de la imagen recibida en la misma videollamada. Además de esto, Sumsub generó posteriormente vídeos deepfake usando para ello una imagen en alta resolución. Con una imagen de este tipo, el resultado es todavía mejor, pero incluso la imagen en directo es suficiente para reproducir con fidelidad los rasgos faciales de una forma totalmente creíble. Y hay que recordar que, en Internet, se pueden encontrar imágenes de este tipo de prácticamente cualquier persona.



El experimento en directo: solo por el peinado, es posible reconocer claramente quién es el redactor del mundo real (abajo a la derecha).



Partiendo de una buena foto, nadie caería en la cuenta de que se trata de un deepfake.

NO, NO ES TU HIJO...

CLONAN CON IA LA VOZ

La policía advierte de que los timadores están usando la inteligencia artificial para clonar las voces de familiares y conocidos. Si recibes un audio o una llamada sospechosa, deberás contrastar primero la información con la persona a la que podrían suplantar la identidad.

Una oleada de usuarios está recibiendo llamadas o mensajes de audio en los que se escucha la voz de algún familiar o compañero de trabajo, pero en realidad es una estafa para conseguir dinero o datos personales. Los expertos aseguran que ya existen herramientas IA que los timadores usan con facilidad y sin conocimientos técnicos.

La voz de compañeros y familiares clonada

Los Mossos d'Esquadra alertan sobre el uso de deepfakes de audio en llamadas telefónicas, mediante la clonación de voz a través de inteligencia artificial, una de las estafas más comunes vinculadas a esta tecnología. A la advertencia se une el Instituto Nacional de Ciberseguridad, que detalla el caso de una víctima que recibió una llamada desde un número desconocido, en la que escuchó la voz de su esposo diciendo: "¡Hola! No te puedo llamar, envíame un mensaje a este número". Sin embargo, al contactar con su pareja a través de su número de teléfono real, descubrió que se trataba de una suplantación de identidad.

José Ángel Merino, director del área de delitos económicos de los Mossos d'Esquadra, señaló en una rueda de prensa que la clonación de voces con IA también se utiliza para estafar a compañeros de trabajo. "Un trabajador de una gasolinera recibe un audio en el que identifica como interlocutor a un compañero de trabajo, que le pide que haga una transferencia de dinero", ejemplifica Merino.

Foto: Depositphotos.com

Si detectas un uso indebido de tus datos, solicita su eliminación a la plataforma o, si es necesario, contacta con la Agencia Española de Protección de Datos.

Herramientas que están al alcance de los estafadores

Existen utilidades que permiten clonar voces con sorprendente facilidad. Una de ellas permite cargar un audio para registrar la voz en la aplicación. Entonces, "puedes escribir cualquier texto para que sea reproducido con esa voz, y el resultado lo puedes descargar en formato MP3", revela a Maldita.es Roberto Carreras, director de marketing de voz en LLYC. Lo más curioso es que el audio original puede durar unos escasos minutos o incluso unos pocos segundos, y ser suficiente para clonar una voz. Aunque la calidad del archivo influye en el resultado, a los estafadores les basta con cualquier grabación.

KIOSKEROS

DE TUS SERES QUERIDOS

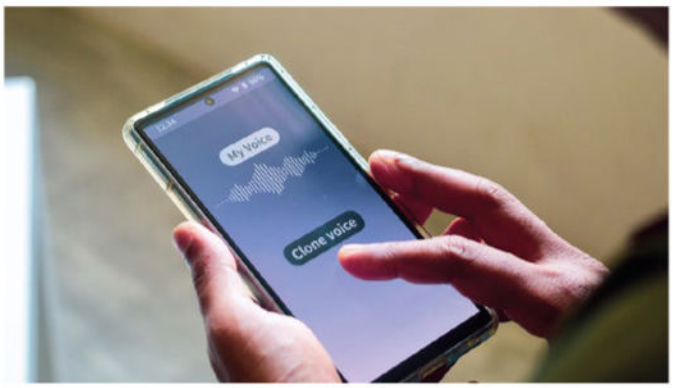
Los timadores suelen obtener estos fragmentos de plataformas como YouTube, Instagram o TikTok, según confirman Carreras y Carmen Torrijos, lingüista computacional y responsable de IA en Prodigioso Volcán.

Cómo actuar ante una sospecha de voz clonada

El Instituto Nacional de Ciberseguridad (INCIBE) comparte cuatro consejos clave para prevenir y responder ante estafas basada en la clonación por IA:

- **Verifica la autenticidad:** si recibes una llamada sospechosa, contacta directamente con la persona cuya identidad podría estar siendo suplantada.
- **Protege tus datos:** nunca facilites información bancaria, personal y otros datos importantes.

Recibes una llamada de un amigo o familiar pidiéndote datos confidenciales o dinero. Parece real porque reconoces su voz, pero ¿y si no son ellos?



Para proteger a los usuarios, también se están desarrollando tecnologías de seguridad biométrica que pueden distinguir entre una voz real y una clonada.

- **No sigas instrucciones sospechosas:** evita descargar aplicaciones o enlaces que lo indiquen.
- **Una palabra clave:** establece una contraseña o palabra clave secreta con amigos y familiares, para confirma su identidad en situaciones dudosas.

Si usan tu voz clonada, INCIBE ofrece estas recomendaciones:

- **Avisa a tus contactos:** informa a conocidos sobre la posibilidad de que reciban audios o llamadas fraudulentas.
- **Bloqueo:** impide de manera definitiva el contacto desde el número que hace la llamada o envía los audios sospechosos.
- **Notifica a las autoridades:** comunica el incidente a la Guardia Civil o la Policía Nacional para su pronta intervención.
- **Revisa tu huella digital:** comprueba detalladamente qué información personal hay disponible sobre ti en Internet.

UNA NUEVA AMENAZA: ¡CHANTAJE EN INTERNET!

CHANTAJE ¡CON FOTOS DE IA!

Los ciberdelincuentes utilizan aplicaciones de inteligencia artificial para crear fotos de jóvenes desnudos y chantajear a los padres. Te contamos cómo proteger a tus hijos.

Si alguien te escribe diciendo que tu hija está prostituyéndose, probablemente al principio pienses que se trata de una broma de muy mal gusto. Pero por desgracia, no lo es. Se trata del chantaje más ruin y sin escrúpulos que se propaga actualmente por Internet. Lo peor de todo es que las víctimas son jóvenes, **apenas tienen posibilidad de defenderse** y se exponen al ridículo y a la maldad como consecuencia del desagradable comportamiento delictivo. ¡Esto puede llegar a destrozar la vida de la víctima! Claro que a los responsables les importa más bien poco. Computer Hoy te explica de qué se trata, cómo puedes protegerte y qué puedes hacer en caso de emergencia.

Fotos falsas de desnudos

El correo electrónico del chantajista no solo contiene el impactante mensaje, sino también un enlace a un perfil en algún sitio de sexo en Internet. Allí encontrarás las correspondientes fotos de la víctima, es decir, ¡de tu hijo o de ti mismo! Los delincuentes han copiado las plantillas de las redes sociales y **han generado fotos de desnudos** a partir de ellas utilizando aplicaciones de IA, y esto no puede reconocerse a simple vista.

En realidad, estas aplicaciones están diseñadas para hacer correcciones de belleza, eliminar objetos superfluos o sustituir fondos. Sin embargo, también se utilizan con fines pornográficos e ilegales. Las llamadas aplicaciones Nudify (ver imagen inferior de la siguiente página) están especializadas en eliminar la ropa de las figuras de la imagen. Y tampoco son difíciles de encontrar; ¡incluso existen como chatbots ilegales en Telegram!

Aunque muchos de los proveedores oficiales prohíben el uso ilegal de apps en sus términos y condiciones, esto sigue

siendo posible. Al fin y al cabo, el servicio no puede comprobar si tienes los derechos de imagen. Y los delincuentes simplemente ignoran las prohibiciones, por supuesto. Hasta ahora, han sido sobre todo los famosos los que han tenido que lidiar con esto; ahora los ciberdelincuentes **se dirigen también a las familias**. ¡Bandas enteras se han especializado en chantajearlas con estas mencionadas falsificaciones de IA!

Cómo funciona la estafa

Los estafadores no necesitan hacer un gran esfuerzo para chantajear a la gente. Simplemente buscan fotos de jóvenes (sobre todo de chicas) en Facebook, Instagram y similares, y utilizan una aplicación para quitarle la ropa y crear rápidamente un perfil adecuado en un sitio sospechoso, a veces incluso incluyendo una traducción automática de texto. Los padres de la víctima reciben entonces un correo electrónico del chantaje, con **un enlace al perfil y una amenaza:** si no pagan, el enlace en cuestión se difundirá en el entorno, tanto de su vida privada como profesional.

Víctimas indefensas

Una vez que las fotografías comprometedoras se encuentran online, es realmente difícil contener su difusión. Y nadie que las vea se parará a pensar o a intentar comprobar si en realidad se trata de falsificaciones elaboradas mediante herramientas de inteligencia artificial.

Si esas imágenes llegan a entrar en el entorno escolar de las víctimas, esto puede destruir la vida de los afectados, porque los adolescentes pueden reaccionar en ocasiones con crueldad. Incluso aunque sepan que son solo falsificaciones, pueden **dar lugar a toda clase de comentarios hirientes** o, incluso, provocar acoso escolar. No servirá de mucho explicar que se trata de fotos falsas que los delincuentes diseñaron con fines de chantaje. El daño a esas alturas ya estará más que hecho.

Así puedes protegerte

Tienes que protegerte para no llegar a esa situación. ¿Cómo? Sobre todo, 'limitando' las fotos de tus hijos en Internet. Asegúrate de que no haya imágenes de cuerpo entero en la Red y que las fotos no muestren a tu hijo de frente. Este tipo de imágenes son especialmente adecuadas para la manipulación mediante IA. Y **restringe lo que es visible** públicamente. En la mayoría de las redes, el círculo de personas que pueden ver fotos puede limitarse a los amigos.

También debes decidir quién está autorizado a etiquetar el perfil de tu hijo y a escribir en los comentarios. Asegúrate de implicar a tus hijos en las medidas de protección. Solo serán cuidadosos con sus fotos si son conscientes de los ciberpeligros y prestan ellos mismos atención al establecer estas restricciones.

¿Suiza es el modelo a seguir?

En Suiza, el chantaje se ha convertido en un asunto político. Una alianza de varios partidos está intentando prohibir las aplicaciones en cuestión. Esto también debería imposibilitar el acceso a las herramientas de IA desde Suiza, y así se evitaría al menos que los escolares manipulasen las fotos. Sin embargo, no impide el chantaje, ya que los autores suelen estar en el extranjero y también podrían eludir estos bloqueos mediante el uso, por ejemplo, de un servicio VPN. Actualmente, no hay planes para bloquear este tipo de aplicaciones en España.

Las penas son severas

Sin embargo, un portavoz del Ministerio Federal del Interior en Alemania nos explicó que la legislación europea vigente ya permite **perseguir estos deepfakes** en muchos casos. Por ejemplo, difamación, violación de los derechos de la persona, distribución de contenidos pornográficos y, dependiendo de la edad de la víctima, pornografía infantil o juvenil son posibles cargos por los que los autores se enfrentan a **penas considerables**. También hay que reconocer que, desgraciadamente, esto es de poca ayuda para los perjudicados.

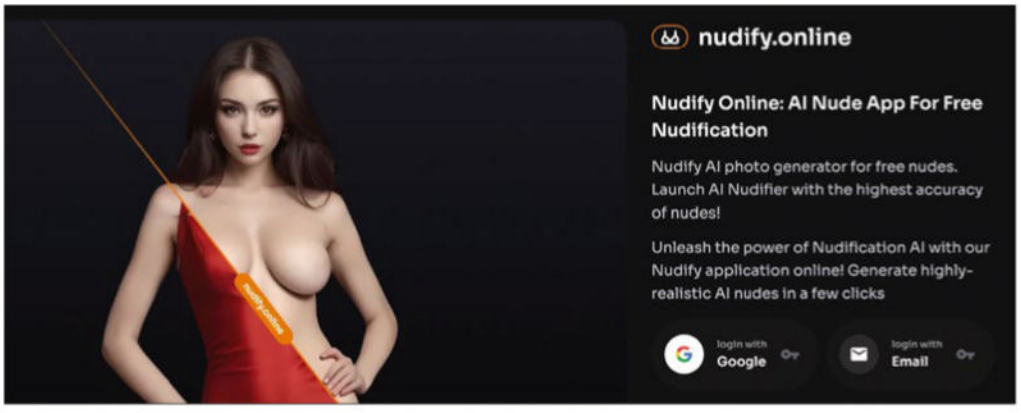
¿Qué puede hacer la víctima?

Si recibes un mensaje de chantaje, denúncialo a la policía lo antes posible. **Guarda todo lo relacionado con el chantaje** y haz capturas de pantalla de la página enlazada. Además, escribe directamente a la dirección de email de la página con el perfil falso para que borren las imágenes lo antes posible.

También es importante que te asegures de hablar con tu hijo sobre el tema y se aconseja que no pagues el dinero exigido, ya que aunque cumplan el trato, los delincuentes pueden volver a intentarlo poco tiempo después. Y, por supuesto, el pago recompensa a los delincuentes.

CÓMO PROTEGER A TUS HIJOS

Para tu hijo adolescente o preadolescente, este chantaje es una de las peores cosas que le pueden pasar. Apenas están aprendiendo a manejar su propio cuerpo y su sexualidad y, de repente, se les **expone públicamente** en un momento tan delicado, cuando más les importa lo que otros piensan de ellos y da igual que las fotos sean falsas. Además, aunque sea improbable que los autores lleven a cabo la amenaza, el miedo está ahí. Por lo tanto, como padre o madre, tienes que estar al lado de tu hijo y estar atento a los cambios de comportamiento. Habla abiertamente con él y apóyale en lo que puedas. También debes buscar apoyo tú mismo, en caso de que ocurra lo peor. Por ejemplo, puedes llamar a la línea de ayuda de **INCIBE** (Instituto Nacional de Ciberseguridad) en el 017, donde podrás describir el incidente y obtener valiosos consejos tanto para ese momento como para el futuro. Otras medidas dependen del comportamiento del menor y de la situación concreta, pero sobre todo ten en cuenta que deben tomarse tras consultar con los expertos.



Las aplicaciones Nudify están disponibles legalmente en Internet. Pero cuidado: quien desnude a personas en fotos ajenas utilizando IA y distribuya los resultados no está cometiendo un delito trivial. Hay penas muy severas.

¿PUEDE ENTRAR MI SMARTPHONE EN EE. UU.?

Si vas a viajar a Estados Unidos, bien sea por trabajo o por ocio, es muy probable que tu parecer haya cambiado un poco respecto al que tenías hace unos meses. Y es que la política del presidente estadounidense Trump ha llevado a que ya **no sean bienvenidos todos los visitantes**. Cada vez se conocen más casos de personas a las que se les ha denegado la entrada, y uno de los motivos puede ser que a los agentes de la patrulla fronteriza no les guste el contenido que puedan encontrar en smartphones y ordenadores portátiles. Por ejemplo, hace algún tiempo, se le denegó la entrada en el país a un científico francés por tener chats en los que se hablaba en contra de los EE. UU. Entonces, ¿es mejor dejar tu smartphone en casa? A continuación, te lo aclaramos.

Endurecimiento fronterizo

El pasado mes de marzo, los ministerios de asuntos exteriores de algunos países agravaron sus recomendaciones para viajar a los Estados Unidos. En estas recomendaciones, se comunicaba que ni tan siquiera un visado o permiso de entrada ESTA válido garantizaría que uno pudiera entrar en el país. Los agentes fronterizos de EE. UU. son una barrera. Estos agentes tienen amplios poderes y pueden registrar dispositivos electrónicos como ordenadores portátiles, tablets o smartphones e, incluso, confiscarlos llegado el caso.

Qué no debes hacer

Lo más importante es no confiar en que los agentes fronterizos no puedan acceder a tu smartphone o portátil solamente porque, para lograrlo, haya que acceder con tu huella dactilar o mediante el reconocimiento facial. No tienen más que sostener el dispositivo delante de tu rostro o invitarte a que sitúes tu dedo en el sensor del teléfono y, en ese momento, ya podrán acceder a todos tus datos.

Hay que ir sobre seguro

¿Qué hay que hacer si viajas a Estados Unidos y quieres reducir el riesgo? El método más simple: llévate contigo, si es posible, **un dispositivo distinto del que utilizas** habitualmente. Para pasar unas cortas vacaciones en los Estados Unidos, seguro que puedes usar un viejo smartphone que tengas por ahí en algún cajón de casa y que ya no uses. Lo primero de todo es limpiarlo bien: existen apps como Secure Erase, SecureWipe o Kshred que pueden borrar la memoria para que no se pueda recuperar nada. Seguidamente restablece el smartphone a los valores de fábrica. Para ello, accede a los Ajustes y podrás encontrar la opción correspondiente; busca algo parecido a ***Restablecer dispositivo*** o ***Configuración de fábrica***. Una vez que hayas borrado todo el contenido de forma segura, lo mejor es que configures la bandeja de entrada, lo más 'vacía' posible, para el correo electrónico. Después, sube unas cuantas fotos inocentes, descarga algunas apps inofensivas y abstente de instalar aplicaciones de mensajería instantánea como WhatsApp. Repite el proceso con los tablets. Esto mismo se aplica, de forma parecida, en el caso de los portátiles que puedas necesitar para trabajar. Usa un programa como CCleaner o similar. En los ajustes de este podrás encontrar la opción ***Borrado seguro*** que lo que hace es sobrescribir repetidas veces la memoria libre del dispositivo con todo tipo de datos aleatorios. Por si pensabas que esto es un poco exagerado: por temor al espionaje, la UE proporciona a sus funcionarios dispositivos especiales que se denominan dispositivos Burner o desechables, y que se destruyen después del viaje. Este tipo de medidas de seguridad se aplican ya desde hace tiempo cuando, por ejemplo, se viaja a China. En caso de que tu viaje sea por motivos de tra-

Todo el que viaje ahora a los EE. UU. tendrá que estar preparado para cualquier circunstancia, incluido el que puedan registrarte tu teléfono móvil. A continuación, encontrarás todo lo que debes saber al respecto.

bajo, lo mejor es que consultes las instrucciones o normativas a seguir con el **departamento de seguridad de tu empresa**.

¿Y qué ocurre con los chats de conversaciones antiguas?

Según la información del servicio de WhatsApp, los mensajes antiguos no se almacenan en los servidores de Meta una vez enviados. Si te decides por instalar WhatsApp nuevamente en el smartphone 'limpio', los chats antiguos únicamente se restaurarán si previamente habías hecho una copia de seguridad de ellos en alguna ubicación. Sin embargo, esto es algo que ya hacen muchos usuarios, aunque siempre puedes pasar por alto esta opción durante la instalación. Otra opción es **usar una tarjeta SIM nueva**, con la que empezar sin ningún tipo de condicionantes. Una vez llegado a tu país de residencia, la puedes volver a cambiar. Como alternativa, puedes usar otras apps de mensajería en EE. UU., como **Signal o Threema**, que ofrecen mayor seguridad.

¿Redes sociales? Mejor no

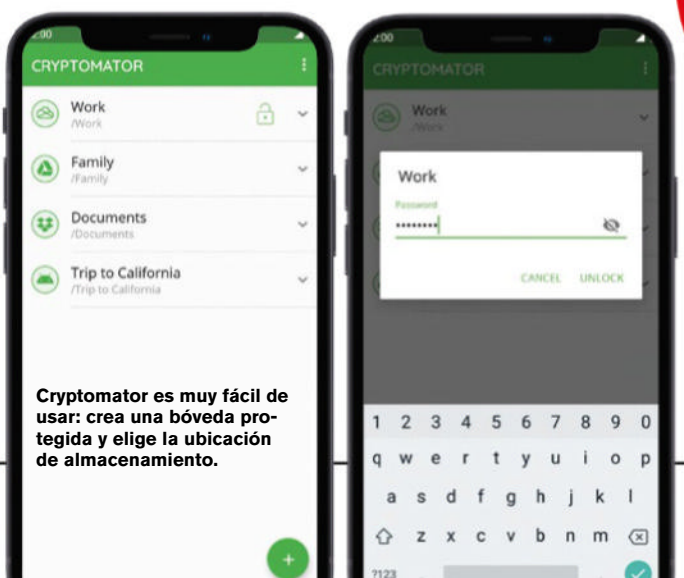
De Facebook a Instagram: las cuentas de las redes sociales proporcionan mucha información sobre tus opiniones, ideología y puntos de vista. Esta información normalmente es de acceso público y es de esperar que esta sea examinada. Si existe la posibilidad de encontrarte alguna sorpresa desagradable en tu muro, lo mejor es no instalar las correspondientes apps. En cualquier caso, si no existen sospechas concretas, no es probable que un agente fronterizo acometa el esfuerzo de iniciar una investigación completa.

El cifrado ayuda

Muchas veces es imposible prescindir de información profesional o privada importante cuando se viaja. Si este es tu caso, siempre puedes guardar dicha información de forma cifrada. Para ello usa apps y software como Axcrypt, Veracrypt o Cryptomator (ver cuadro), emplea contraseñas complejas para conseguir el mayor nivel de seguridad y no uses los sistemas de reconocimiento biométrico. Los agentes tendrán que solicitarte que introduzcas la clave personalmente, y quizás en ese momento la hayas olvidado de manera fortuita.

CUANDO VIAJES, CIFRA BIEN LOS DATOS

La herramienta de cifrado Cryptomator puede proteger tus datos privados y profesionales frente a las miradas indiscretas. Funciona tanto en PC como en smartphones, aunque la aplicación es de pago. Sin embargo, cuentas con un periodo de prueba gratuito de 30 días, lo que es un tiempo más que suficiente para la mayoría de los viajes. Pasado ese tiempo, no podrás cifrar archivos nuevos, pero seguirás pudiendo acceder a los datos que hayas almacenado encriptados. Una vez realizada la instalación, especifica la ubicación de almacenamiento de tu bóveda de datos cifrada. Esta puede almacenarse tanto en el dispositivo como en la nube. En este espacio, se hará una copia de seguridad de tus archivos secretos. Por otro lado, aunque la nube que uses probablemente sea estadounidense, como es el caso de Google o Microsoft, los datos únicamente se podrán descifrar con tu contraseña.



Cryptomator es muy fácil de usar: crea una bóveda protegida y elige la ubicación de almacenamiento.

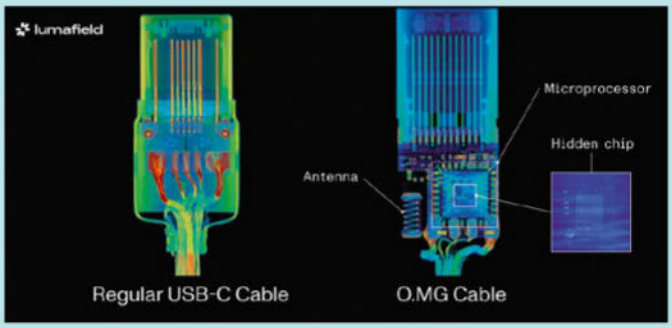
Define una contraseña que solamente tú conozcas. ¡No hagas uso del reconocimiento biométrico!

KIOSKEROS

HARDWARE MALICIOSO

ESTE CABLE TE ESPÍA

¿Los virus únicamente provienen de Internet? Pues desafortunadamente no. Debes saber que el hardware también puede ser la puerta de entrada para curiosos y ciberdelincuentes.



Así es como se ve un cable manipulado bajo la máquina de rayos X de Lumafield: a la derecha, puede verse el chip integrado y la antena de radio.

Siempre que pensamos en los ataques de los hackers, pensamos en el ámbito del software, en forma de un código malicioso que se cuela en el ordenador al navegar por una **web que ha sido manipulada**. Para luchar contra este tipo de amenazas, los programas antivirus de Norton y otros proveedores ya ofrecen una protección bastante fiable. Pero ¿qué pasa si el malware ya está en tu hardware y no eres consciente?

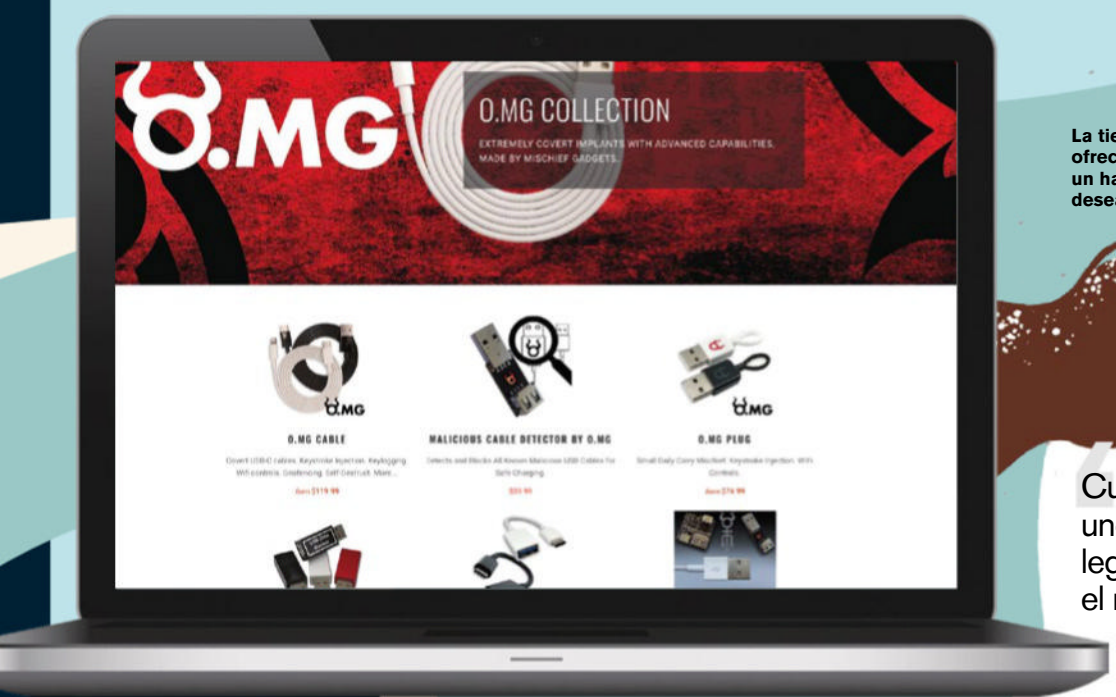
Una empresa muy particular...

Existen muchos dispositivos que pueden usarse para atacar ordenadores y móviles, y detrás suele haber fabricantes que venden estos productos de forma legal desde hace años. Uno de ellos es la tienda estadounidense Hak5. Esta empresa de San Francisco muestra orgullosa en su web las numerosas referencias a sus productos en la prensa, y resalta que han aparecido en diversas películas y series como 'Mr. Robot' o 'Superman'. Oficialmente, estos dispositivos se usan para **los denominados 'pen tests'** o pruebas de penetración. Es decir, los expertos en seguridad los emplean para comprobar si un entorno informático es vulnerable a los ataques. Sin embargo, también los pueden usar los ciberdelincuentes para perpetrar los suyos propios.

... con un cable especial

Uno de estos productos es el cable 'O.MG'. A simple vista, se parece a uno de los cables USB normales que se usan para cargar el móvil o conectar otros dispositivos a un portátil o PC. Sin embargo, aunque su apariencia externa es completamente normal, en uno de sus extremos incorpora una tecnología adicional. En su interior dispone de un chip y una antena, que no podrás encontrar en los cables corrientes. Si un ciberdelincuente tiene acceso a una sala o dispositivo desatendido, podría reemplazar un cable ya existente por este otro. La víctima no percibiría nada extraño, porque la función básica del cable es, en principio, la habitual. Así que, podría seguir funcionando el tiempo necesario de la forma tradicional, hasta que el atacante lo 'despierte' y active sus funciones maliciosas.

Pero antes de usarlo, **hay que preparar el cable** de forma adecuada. Esto puede lograrse mediante un dispositivo y un sencillo lenguaje de programación. Luego, la tecnología que integra



La tienda Hak5.org ofrece todo lo que un hacker puede desear.

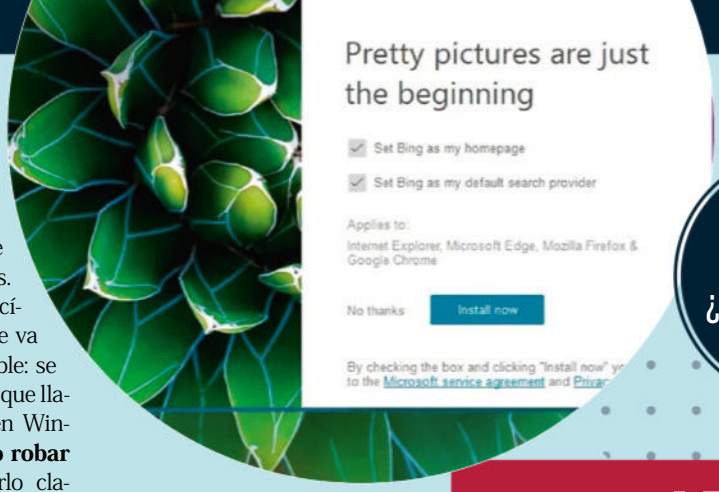
> Cuesta creer lo que uno puede comprar legalmente en el mercado.
>
> **Dirk General-Kuchel**
> Redactor

configurará su propia red inalámbrica para que pueda recibir las órdenes. El atacante definirá específicamente el malware que va a poner en marcha el cable: se puede simular un teclado que llama a otros programas en Windows, **abrir sitios web o robar contraseñas**. Para dejarlo claro: el ordenador estará completamente a merced del delincuente.

La inversión que los atacantes tienen que realizar para adquirir un cable de este tipo no es pequeña; solamente el cable cuesta al menos 120 $, a lo que hay que añadir el dispositivo de programación. Las víctimas más propicias para este tipo de ataque se encuentran en el ámbito de la política y los negocios. Dado que se trata de un tipo de ataque bastante especializado, el software antivirus no suele ser eficaz contra ellos. Además, este cable permite asumir el control de los smartphones, que por lo general no suelen disponer de ningún software de protección.

Cómo puedes protegerte

Para reconocer estas amenazas, la empresa norteamericana Lumafield utiliza una máquina de rayos X, que ha sido desarrollada por ella misma para descubrir este tipo de cables. El portavoz de la compañía, Jon Bruner, lo explica en una entrevista a Computer Hoy: "Ya hay algunos fabricantes que usan nuestra tecnología, y escanean de manera predeterminada los componentes que se les suministran en busca de anomalías de este tipo". Según Bruner, también hay empresas que utilizan estas **máquinas de rayos X** para analizar los dispositivos de sus empleados más importantes cuando regresan de sus viajes de negocios por el extranjero. Por su parte, los usuarios normales que no se sientan seguros tienen una opción muy sencilla: desechar el cable actual y usar uno nuevo.



MUY BONITO, PERO... ¿TAMBIÉN MUY PELIGROSO?

¿ESPIONAJE O IMÁGENES CHULAS?

¿Te gustan las bonitas imágenes de fondo del buscador Microsoft Bing? Entonces, quizás te hayas alegrado al descubrir que la app Bing Wallpaper ya se puede descargar de forma gratuita desde la tienda de Microsoft. No obstante, el experto en seguridad estadounidense Rafael Rivera se pregunta por qué está poniendo Microsoft tanto empeño para una aplicación que lo único que hace es cambiar el fondo de pantalla de Windows. Después de estudiarlo más de cerca, ahora cree que la empresa matriz de Windows está colando a los usuarios, mediante este método, un software no deseado y además espiando a los clientes. ¿Es esto cierto?

Podría haber algo

Rivera señala que la aplicación Wallpaper instala también Bing Visual Search, una herramienta que sirve para buscar en Internet con imágenes o fotos que se arrastran a un área de búsqueda, en lugar de con los términos clave habituales. El motor de búsqueda ofrece así resultados que se ajustan o están relacionados con las imágenes arrastradas. Sin embargo, los resultados que se ofrecen no están basados en Google u otros motores de búsqueda, sino en el propio motor Bing de Microsoft. Este es el método que la empresa intenta usar para reforzar su posición en el mercado de los buscadores. Pero ¿se trata realmente de software malicioso? Computer Hoy pidió la opinión de los expertos de Norton, y estos contestaron que no. El equipo de Norton clasifica la aplicación Bing Visual Search como un PUP (Potentially Unwanted Program), es decir; un programa potencialmente indeseable. Todo aquel que no quiera llevar a cabo cambio alguno en sus procesos de búsqueda habituales simplemente debería desmarcar todas las casillas en el momento de la instalación.

Pero aún hay más

Las acusaciones de Rivera van un poco más allá. Según sus análisis, la aplicación husmea también entre las cookies de los usuarios que han sido recogidas por otros navegadores como Chrome o Firefox . Luego, las desencripta. Este sería un comportamiento clásico del malware y lo utilizan habitualmente los atacantes para hacerse pasar por otra persona al navegar por sitios web. Al ser preguntados por la revista digital 'The Register', Microsoft publicó un desmentido poco convincente, cuya redacción de por sí ya intrigaba un poco. La empresa estadounidense subrayó que no se descifraban "todas las cookies". ¿Así que algunas sí que se descifran? Resulta también poco tranquilizador que, en su comunicado, Microsoft no haga mención a las cookies de Firefox y solo nombre las de Edge y Chrome.

Mejor ir con cuidado...

Lo que al final se le queda a uno es una extraña sensación incómoda de desconfianza. De momento, la opción más segura es renunciar a las bonitas fotos de Microsoft y utilizar tus propias fotos en su lugar, que seguro que tienes suficientes.

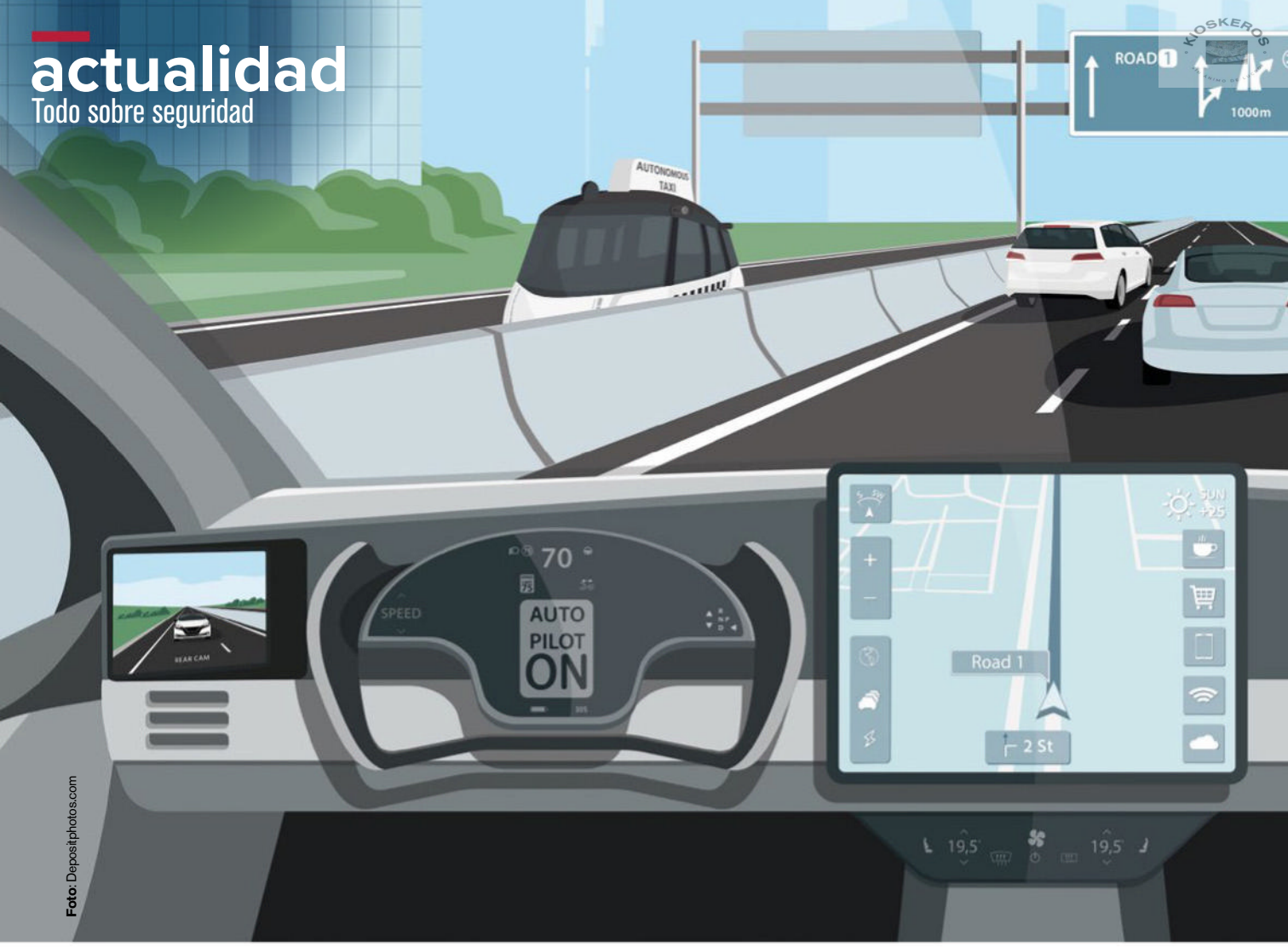


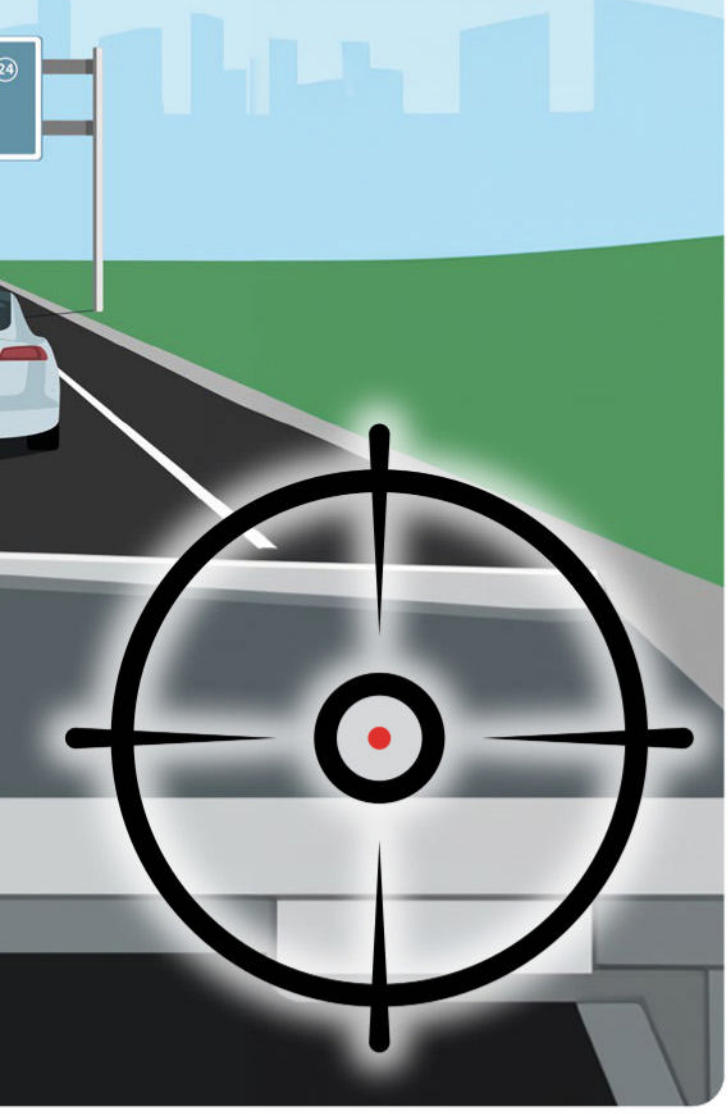
Foto: Depositphotos.com

EL COCHE EN EL PUNTO DE MIRA DE LOS HACKERS

Los vehículos de hoy en día se asemejan cada vez más a ordenadores sobre ruedas. Un experto nos explica qué significa esto para los conductores, en términos de ciberseguridad.

Malware, ransomware o phishing; estar conectado implica estar expuesto a las amenazas de Internet, pero ya no se trata solamente los PC, smartphones y electrodomésticos inteligentes los que se conectan a la Red. Ahora, cada vez hay más coches conectados y el desarrollo constante de los vehículos los está convirtiendo en ordenadores con ruedas, que además se comunican con el mundo exterior a través de la telefonía móvil. Entonces, ¿existe también aquí el peligro de sufrir ataques provenientes de delincuentes informáticos? ¿Qué consecuencias podrían tener este tipo de ataques? ¿Y de qué manera pueden protegerse los conductores? Computer Hoy ha conversado sobre todo esto con Ronen Smoly, Director general de PlaxidityX, un especialista en el sector de la ciberseguridad para el automóvil y sus respuestas resultan muy útiles para todos aquellos usuarios interesados en este tipo de tecnología. Aquí puedes verlo:

Sr. Smoly, los coches son cada vez más inteligentes. ¿Implica esto un aumento de las posibilidades de sufrir un ciberataque? Por supuesto. Durante la última década se han desarrollado nuevas tecnologías en el campo de la automoción, y los vehículos son cada vez más una extensión de nuestros propios hogares. Los coches de hoy en día vienen perfectamente equipados con una conexión a Internet, software de todo tipo y hasta poseen cámaras que pueden grabar dentro y fuera del vehículo. Cuanto más conectado esté un vehículo, mayor será también el riesgo de sufrir un ataque informático.

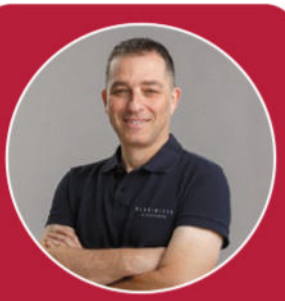


¿A qué amenazas concretas se enfrentan los conductores?
Existen varias. La más peligrosa de ellas es que alguien pueda piratear el vehículo y dañar el sistema de frenado o el airbag. De hecho, esto es relativamente sencillo de lograr una vez que ya se ha entrado en el sistema. Para que se entienda mejor: hackear un vehículo es diez veces más fácil que hackear un móvil. Por otro lado, la privacidad del conductor y los ocupantes del vehículo también está en compromiso, puesto que alguien podría hackear el vehículo, pinchar las cámaras internas y espiar a sus ocupantes. El ciberdelincuente también podría lograr acceder a los datos que se almacenan en el coche, como los de ubicación, contactos o el mismo registro de llamadas. Estos serían algunos de los riesgos más inmediatos.

Entonces, ¿es frecuente que los vehículos sufran ciberataques?
Afortunadamente, todavía no hemos sufrido ciberataques de envergadura que pudieran suponer un riesgo para la seguridad vial. Sin embargo, somos una empresa centrada en la ciberseguridad y observamos continuamente en la Dark Web intentos de hackear los vehículos. Podría incluso decirse que existe una auténtica competición entre los hackers, para ver quién es el primero en hackear los nuevos modelos de vehículos que van apareciendo en el mercado. Por fortuna, en la mayoría de las ocasiones, se trata de los llamados white hat hackers (hackers de sombreo blanco), es decir, hackers éticos que intentan hackear los vehículos para advertir a los fabricantes sobre los puntos flacos de sus sistemas. De todas formas, estos intentos de ciberataque rara vez llegan a hacerse públicos, puesto que a los fabricantes no les interesa que esto ocurra. ¿Quién no tendría serias reticencias a la hora de adquirir un vehículo sabiendo que docenas de hackers han intentado piratearlo?

¿Cómo sé si mi coche está a salvo de sufrir ciberataques?
Al contrario de lo que sucede con las normativas y directrices de seguridad en caso de colisión, aún no existe una guía clara de instrucciones para los consumidores en materia de ciberseguridad. Mientras que los usuarios pueden conocer de forma transparente el nivel de protección que ofrecen sus vehículos en caso de colisión, gracias a organizaciones independientes que evalúan el comportamiento del vehículo en base a un baremo de estrellas, no existe por ahora un sistema similar para la seguridad digital de estos mismos vehículos. El programa de seguridad para automóviles NCAP (New Car Assessment Program) tiene la voluntad de cambiar esta situación dentro de dos o tres años, y otorgar también una calificación en materia de ciberseguridad de los vehículos. Sin embargo, en el caso de los coches nuevos, podemos tener la certeza de que ya se aplican medidas de ciberseguridad. Esto es así porque la norma UNR155 de la UE obliga a que todos los nuevos modelos que salgan al mercado a partir de julio de 2024 deben cumplir con determinadas normas en materia de ciberseguridad. Además de la protección básica gratuita que incluya el vehículo, los consumidores podrán en breve adquirir soluciones de ciberseguridad personalizadas, como si se tratara de una suscripción antivirus para su vehículo. Se prevé que los usuarios podrán acceder a estos servicios en uno o dos años.

Actualmente, ¿qué consejos puede dar a los consumidores?
El único consejo que se puede dar a los usuarios de vehículos es que se informen en su concesionario sobre las medidas de ciberseguridad del coche. Hemos integrado nuestras soluciones en más de 70 millones de vehículos y estas ofrecen una protección eficaz frente a los ciberataques. También es siempre importante conocer cuáles son las fuentes potenciales de peligro. Por ejemplo, una aplicación infectada en un teléfono móvil podría permitir que los hackers accedan de forma remota al vehículo si el smartphone en cuestión está conectado al vehículo. Es por este mismo motivo que los consumidores deberán limitar el acceso de terceros, por ejemplo a la hora de vincular apps, y comprobar y supervisar los permisos de las aplicaciones para, de esta forma, poder reducir al máximo el riesgo de que se produzca un uso no autorizado de la información.



Ronen Smoly
CEO de PlaxidityX

ACERCA DE PLAXIDITYX

Ronen Smoly es el CEO de PlaxidityX. Fundada en 2014 bajo el nombre de Argus Cyber Security Ltd, la empresa está especializada en soluciones de ciberseguridad para el sector de la automoción, y ofrece soluciones integrales de seguridad para vehículos conectados. Desde el año 2017, PlaxidityX es una filial de Continental AG. La sede central de la empresa se encuentra en Tel Aviv, Israel.

KIOSKEROS

'SU PAQUETE NO HA PODIDO SER ENTREGADO'

CUIDADO, SUPLANTACIÓN DE EMPRESAS DE LOGÍSTICA

Un nuevo fraude aprovecha el pretexto de una supuesta entrega de paquetes realizada para engañar a los usuarios. Este tipo de estafa, que suele intensificarse en épocas de alta actividad de compras online, ha evolucionado con nuevas estrategias para parecer más creíble.

Desde hace unos años, los estafadores han encontrado un filón en las notificaciones relacionadas con los paquetes que no pueden ser entregados a través de los servicios de mensajería. Estas campañas, que **suelen propagarse por email o SMS**, se encuentran especialmente activas en periodos en los que los usuarios realizan muchas compras online, como las semanas previas a Navidad o los días de rebajas, por lo que convienen estar muy atentos en esas fechas.

Foto: ESET

En el mensaje fraudulento, se incluye el texto 'iEntrega del paquete suspendido!' como reclamo y aviso.

Además, la compañía ESET alerta ahora de una nueva campaña fraudulenta que emplea este mismo gancho para captar nuevas víctimas, replicando una estrategia previamente identificada. En esta ocasión, los estafadores evitan mencionar explícitamente el nombre de una empresa de logística, pero incluyen un logotipo que se podría relacionar visualmente con la empresa GLS.

Las diversas fases del fraude

En el correo que la víctima recibe, es posible comprobar que se le informa de la supuesta entrega de un paquete que no ha podido ser realizada, sin especificar la empresa que lo envía ni su contenido. Además, se añade únicamente una foto genérica y un **código de seguimiento falso**. Igualmente, el remitente del correo no parece estar asociado a ninguna empresa de transporte conocida y, aunque todo esto ya nos debería hacer sospechar que estamos ante un intento de engaño, son

muchos los usuarios que en ese momento están esperando recibir un paquete y hacen caso omiso a las señales sospechosas.

Cabe destacar que los creadores de esta campaña no han puesto demasiado esfuerzo en darle al correo una apariencia demasiado profesional. En su lugar, han utilizado mensajes y plantillas genéricas con el único propósito de guiar al usuario a través de las distintas secciones preparadas, buscando **otorgar de mayor credibilidad al engaño**. Así pues, se puede observar que al usuario se le presentan una serie de pantallas en las que se explican los supuestos motivos por los que aún no le ha sido entregado su paquete. Se le indican también los gastos que conlleva volvérselo a enviar y se le formulan una serie de preguntas para **programar una segunda entrega**.

Obviamente, estas pantallas representan solo una fase previa, cuyo objetivo es engañar al usuario para que proporcione la información valiosa para los estafadores. En este caso, los datos solicitados están relacionados con la tarjeta de crédito de la víctima, bajo el pretexto de reprogramar la entrega de un paquete que, en realidad, nunca existió.

Podría parecer que el único propósito de esta campaña es robar los datos de las tarjetas de crédito de los usuarios que, confiados, los introducen en el formulario fraudulento. Sin embargo, los estafadores ya poseen esa información, obtenida previamente a través de emails y sitios web falsos que imitan a una empresa de transporte. Con estos datos, lo que podrán hacer es realizar compras o contratar servicios a nombre de la víctima.

En este caso particular, al analizar los dominios utilizados en la campaña fraudulenta, se observa que los datos robados se emplean para suscribir a las víctimas a un servicio de streaming de películas y series con un coste mensual de 57,95 €. Además, en las propias páginas webs donde se instruye a los usuarios sobre cómo recibir el supuesto paquete, se menciona también en letra pequeña que no existe ninguna relación con la compañía de transporte GLS.

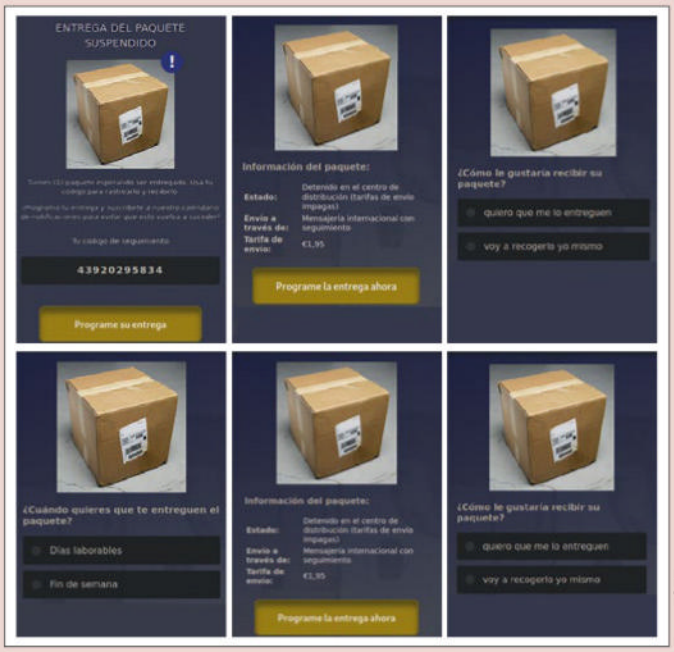


Foto: ESET

La víctima es conducida por una serie de pantallas que, bajo el pretexto de reprogramar la entrega, justifican la supuesta falta de recepción del paquete.

Este tipo de estrategias son comunes en empresas que operan en un área gris de la legalidad. Suelen utilizar señuelos llamativos, como la **supuesta entrega fallida** de un paquete que no ha llegado a su destino, para captar la atención de los usuarios y persuadirlos de que introduzcan los datos de pago. De este modo, los suscriben a servicios que no hubieran contratado voluntariamente, ya sea porque no los necesitan o por su elevado coste. Por todo ello, es fundamentar no dejarse llevar por la urgencia y revisar cuidadosamente cualquier correo o mensajes SMS que informe sobre problemas en la entrega de un paquete. Antes de actuar, es recomendable siempre **verificar la legitimidad del aviso**, por ejemplo, acudiendo directamente a la web del comercio donde se realizó la compra y comprobando el estado del pedido.

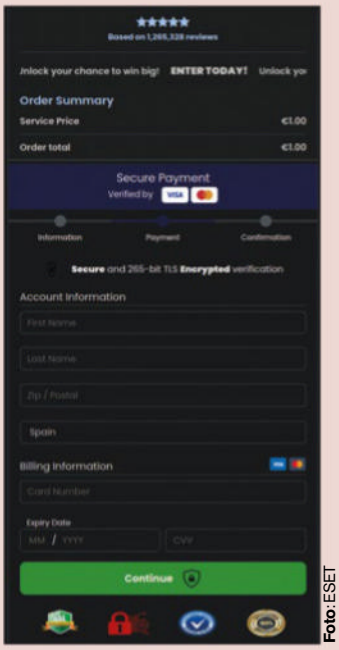


Foto: ESET

En la última parte del engaño, los delincuentes solicitan a la víctima información de su tarjeta de crédito.

DELGADO POR 90 EUROS

Con una inyección a la semana los kilos desaparecen. Sin embargo, todo esto implica también un desembolso de dinero bastante elevado, y muchas personas prefieren buscar en la red oscura...

Un producto milagro para adelgazar de la Darknet? Un reciente estudio ha revelado que en Internet se pueden conseguir de forma clandestina fármacos adelgazantes famosos como **Wegovy o Mounjaro** por una fracción del precio oficial, pero los chollos suelen tener sus inconvenientes y hasta pueden ser peligrosos. Los expertos ya han puesto el grito en el cielo: ¡son falsificaciones, son ineficaces e, incluso, pueden llegar a ser letales! Además, el que compre en la red oscura (Darknet) no solo pone en riesgo su salud, sino que también se arriesga a sufrir una sanción económica.

La demanda se ha disparado

La locura por los productos milagro contra el sobrepeso ya se ha desatado. Cada vez son más las personas que demandan medicamentos que les puedan hacer perder peso, pero este bum tiene un coste y los pacientes que toman de forma legal el fármaco Wegovy tienen que desembolsar unos 300 € para el tratamiento mensual. Sin embargo, en la red oscura, estos productos pueden conseguirse por apenas 85 €. En un análisis realizado por el equipo de investigación de Cybernews en colaboración con el portal sobre salud Healthnews.com, los expertos encontraron 23 de estos productos en los principales mercados de la Darknet.

Ademas, se distribuyen a todos los rincones del mundo, principalmente **desde ubicaciones de Europa, Estados Unidos e India**. El medicamento más popular, con diferencia, es Semaglutida, con más de 1.000 pedidos encontrados solo en estas 'plataformas oscuras. El resto de fármacos, tan en boga últimamente, también se venden en grandes cantida-

KIOSKEROS

Foto: Depositphotos.com

Este es el aspecto que tiene el medicamento original del fabricante Novo Nordisk, con su envase característico y sus certificaciones oficiales.

des. Aquí tienes ahora la lista de precios del 'lado oscuro':

- **Wegovy:** se trata de un fármaco que, al igual que sucede con el más conocido Ozempic, también ha sido autorizado por la Agencia Española de Medicamentos y Productos Sanitarios (AEMPS) para luchar contra la obesidad. Ambos medicamentos contienen el mismo principio activo conocido como semaglutida. El tratamiento mensual cuesta, por el cauce legal, entre 200 € y 300 €. En algunos sitios de la Darknet, se ofrece el (supuesto) principio activo por unos 85 €.
- **Mounjaro:** este medicamento del fabricante Eli Lilly contiene el principio activo de nombre tirzepatida, que se puede conseguir de manera legal por un desembolso mensual de unos 300 €. Sorprendentemente, los expertos encontraron en la Darknet este producto a un precio más elevado incluso que la opción legal, a partir de unos 460 €.
- **Saxenda:** el coste mensual de este fármaco que incorpora el principio activo de nombre liraglutida es de aproximadamente 300 €, pero en la Darknet se puede conseguir por un precio aproximado de 80 €.

¿Más barato? No tiene por qué

Comprar en la Darknet cuesta aproximadamente la cuarta parte, si se compara con el precio del mercado legal. Los que esperen precios más bajos deben saber que en EE. UU., por ejemplo, los precios oficiales triplican los de España. Además, hay que recalcar que, dado que la demanda es alta, como en el caso del fármaco Mounjaro, uno puede encontrar precios **incluso superiores a los habituales**. Por si esto fuera poco, en España estos medicamentos se dispensan con receta médica, algo que en la Darknet a nadie importa.

Problemas en la aduana

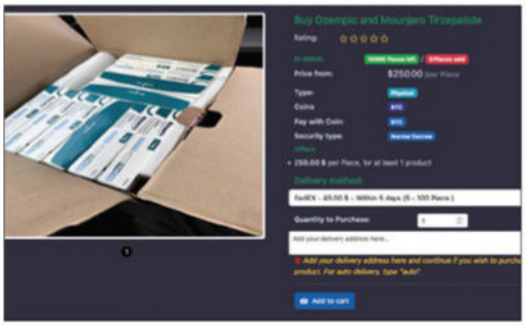
Los precios y la aparente facilidad para acceder a estos fármacos son toda una tentación, pero los expertos nos advierten: los productos que encontramos en la Darknet pueden ser falsificaciones o ser peligrosos para la salud. La doctora Suneye Koohsari, una especialista neoyorquina en el tratamiento de la obesidad declara: "Estos medicamentos no pasan ningún control sanitario. El riesgo de contaminación, dosificación incorrecta y posibles efectos secundarios potencialmente letales es muy alto".

Adquirir estos productos en la Darknet también puede acarrear problemas legales con las autoridades. La situación más probable en estos casos es que los medicamentos falsificados sean interceptados en la aduana y, a continuación, destruidos. Esto ocurriría incluso aunque fueran los originales, puesto que no está permitida su adquisición sin receta, y mucho menos desde países fuera de Europa.

Potencialmente letales

Los expertos analizaron las reseñas de los clientes que han adquirido estos productos en la Darknet. Sin embargo, resulta complicado verificar su autenticidad. De 387 reseñas, únicamente diez de ellas eran negativas. Uno de los compradores informó acerca de un caso grave sobre una reacción autoinmune que le ocasionó una pérdida severa de visión.

Michaela Frank, responsable de comunicación del fabricante Novo Nordisk, advierte que **no se puede determinar lo que contienen las jeringuillas** sin realizar un análisis químico completo. "Existen falsificaciones que son visualmente indistinguibles de los productos originales". Sin embargo, si estas contienen insulina de acción rápida, esto podría tener consecuencias potencialmente letales. La única forma de garantizar la seguridad, subraya, es adquirir los medicamentos en la farmacia de toda la vida.



Una búsqueda en la Darknet nos muestra, en cuestión de minutos, multitud de ofertas para adquirir Ozempic.

En muchos casos, los precios detectados eran prácticamente iguales a los oficiales de las farmacias.

PROTEGE TU PRIVACIDAD

CÓMO CREAR UN CORREO PARA REGISTRARTE SIN

Las direcciones de email desechables protegen tu correo principal y evitan el spam. Estas plataformas en línea generan correos temporales que te permiten registrarte en sitios web sin revelar tu email real, manteniendo tu bandeja de entrada limpia y segura.

El correo electrónico es uno de los datos personales más importantes, ya que no solo te permite identificarte en múltiples servicios, sino que también juega un papel fundamental en la privacidad al navegar por Internet. Si has usado tu email en diversas plataformas, es probable que hayas recibido **spam o mensajes no deseados**, ya que muchas empresas lo emplean para enviar publicidad. En muchos casos, al registrarte en un sitio web, tu correo se agrega automáticamente a listas de distribución, lo cual empeora si el sitio es fraudulento.

Para evitar esto y no saturar tu bandeja de entrada ni consumir almacenamiento innecesario, una buena opción es usar correos temporales para recibir códigos de verificación u otros **datos puntuales durante el registro**. A continuación, te mostramos cómo crear un correo temporal con algunas de las herramientas más popular y fiables.

Un servicio rápido y sencillo

Una cuenta de correo desechable se crea de forma automática o con un simple clic, sin necesidad de registro. Al generarse, se asigna una dirección temporal que puedes usar para registrarte en sitios web. Los mensajes que lleguen a esa dirección aparecerán en una bandeja de entrada del propio servicio. Tras un tiempo limitado, que varía según la plataforma, la dirección y **los mensajes se eliminan automáticamente** para proteger tu privacidad.

LA IMPORTANCIA DE LAS **CUENTAS** DE CORREO ELECTRÓNICO **DESECHABLES**

Hoy en día, muchas páginas web solicitan tu correo electrónico para acceder a períodos de prueba gratuitos o para enviarte un código de verificación que demuestre que eres una persona real y no un bot. Los servicios de correos electrónicos desechables ofrecen una solución práctica a este problema. Funcionan creando direcciones aleatorias a las que puedes acceder temporalmente, como si fueran tu correo principal. La diferencia entre unos y otros radica principalmente en el tiempo de uso: algunas plataformas eliminan la dirección en solo diez minutos, mientras que otras permiten mantenerla activa durante varias horas o incluso un día completo. En resumen, una dirección de correo desechable es útil en muchas situaciones, como por ejemplo:

- Solicitar tarjetas de puntos o fidelidad sin comprometer tu dirección de correo real.
- Probar aplicaciones o páginas web de forma segura, si eres desarrollador o tester.
- Crear cuentas secundarias para gestionar perfiles en redes sociales u otras plataformas digitales de manera organizada.
- Evitar compartir tu correo principal y así mantener limpia tu bandeja de entrada.
- Descargar recursos gratuitos (ebooks, plantillas, etc.) que requieren registro.
- Participar en sorteos o encuestas sin tener que quedar suscrito a listas publicitarias.
- Acceder a contenido restringido que únicamente exige una verificación inicial.

TEMPORAL RIESGOS

TEMPMAIL, UNA NUEVA DIRECCIÓN CADA 10 MINUTOS

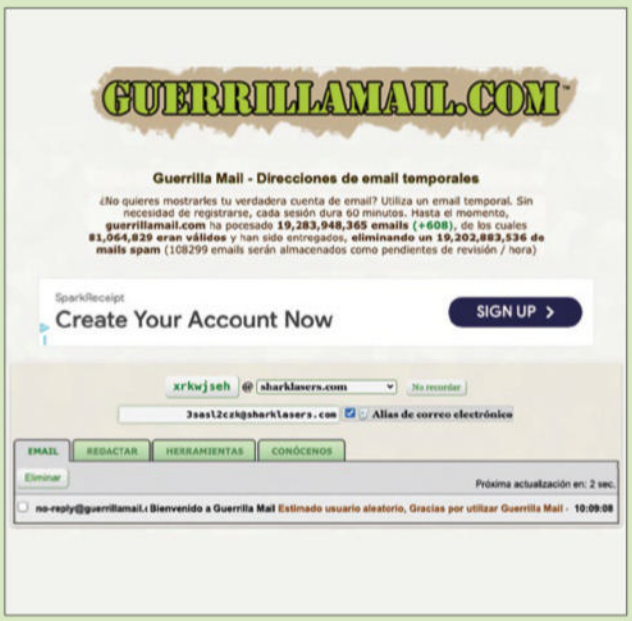
Si quieres probar un servicio web sin usar tu correo principal, TempMail es una excelente opción. Esta herramienta gratuita genera una dirección de correo temporal sin necesidad de registro. La dirección cambia cada 10 min y puedes copiarla, actualizarla, cambiarla o eliminarla fácilmente. La bandeja de entrada de esta plataforma muestra el remitente, asunto y contenido de los mensajes, como cualquier servicio de correo, y es ideal para registrarte en sitios web que requieren verificación adicional para activar una cuenta o para aquellas tiendas online que piden un correo para poder beneficiarte de sus ofertas (lo que a veces desemboca en una avalancha de spam). Además, TempMail permite crear direcciones personalizadas y eliminar cuentas temporales antes de que expiren. También ofrece una app gratuita para iOS y Android.

Página web: temp-mail.org/es

GUERRILLA MAIL

Guerrilla Mail es una herramienta online muy popular para crear direcciones de correo temporales, que resulta ideal a la hora de proteger tu privacidad y evitar el spam al registrarte en sitios web poco fiables. Aunque permite generar direcciones de forma rápida y aleatoria, también ofrece la posibilidad de personalizar el nombre de usuario y elegir entre varias extensiones de dominio disponibles. A diferencia de otras plataformas similares, Guerrilla Mail no hace que las direcciones caduquen automáticamente después de un tiempo fijo. En su versión actual, todos los correos entrantes se mantienen almacenados durante una hora completa. Esto significa que cuando recibes un correo en Guerrilla Mail, queda guardado en espera hasta que lo revises. Si alguien accede a la bandeja de entrada, el sistema buscará nuevos mensajes y, si encuentra alguno, lo moverá inmediatamente a la bandeja de entrada del usuario. Sin embargo, si un correo permanece sin ser revisado durante más de una hora, se eliminará automáticamente. Una vez que el mensaje está en la bandeja de entrada, permanece disponible durante otra hora o hasta que el usuario decida eliminarlo manualmente.

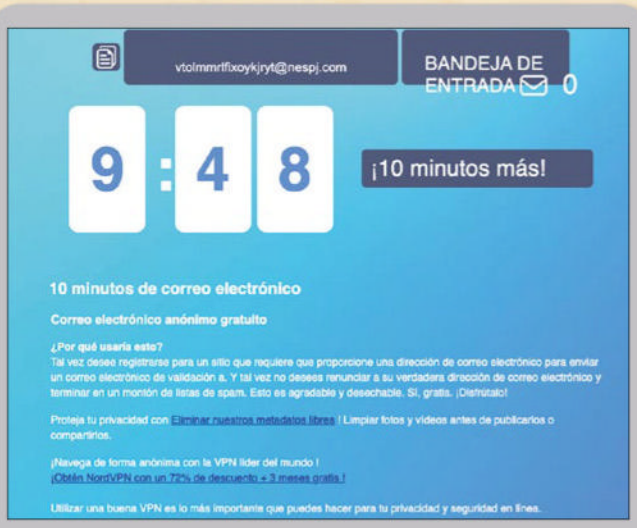
Página web: www.guerrillamail.com/es



YOPMAIL

Esta es otra opción muy popular para crear cuentas de correo electrónico temporales sin necesidad de registro. Su funcionamiento es sencillo y práctico: basta con introducir cualquier nombre de usuario en el sitio web para acceder a una bandeja de entrada temporal, sin necesidad de contraseñas ni procesos de verificación. Las direcciones de correo creadas con YOPmail se conservan durante un período de 8 días, y es posible extender su validez por otros 8 días adicionales si se desea mantener el acceso a los mensajes por más tiempo. Una de sus principales ventajas es la posibilidad de personalizar el nombre de la dirección, lo que facilita su uso en registros específicos. Además, YOPmail ofrece múltiples dominios alternativos, una función especialmente útil para eludir restricciones de páginas web que bloquean correos generados por servicios temporales. Es una herramienta práctica, rápida y eficaz para evitar el spam y proteger tu correo principal.

Página web: yopmail.com/es



10 MINUTE MAIL

Esta es una herramienta rápida y sencilla que permite crear una cuenta de correo electrónico temporal con una duración inicial de 10 min. Resulta muy útil para quienes necesitan una dirección de correo momentánea para realizar tareas puntuales, como registrarse en un sitio web o recibir un código de verificación. No requiere registro ni datos personales, lo que garantiza la privacidad y el anonimato. Al acceder al servicio, se genera automáticamente una dirección de correo junto con una bandeja de entrada visible en la misma página. Allí podrás ver los mensajes recibidos en tiempo real. También se muestra un contador que indica cuánto tiempo queda antes de que la dirección expire. Si necesitas más tiempo, puedes extender la duración por otros 10 min con un simple clic de ratón. Una vez que el contador llega a cero, tanto la dirección como los correos almacenados se eliminan de forma automática, sin dejar ningún rastro.

Página web: 10minutemail.com

FAKE MAIL GENERATOR (EMAIL TEMPORAL GRATIS)

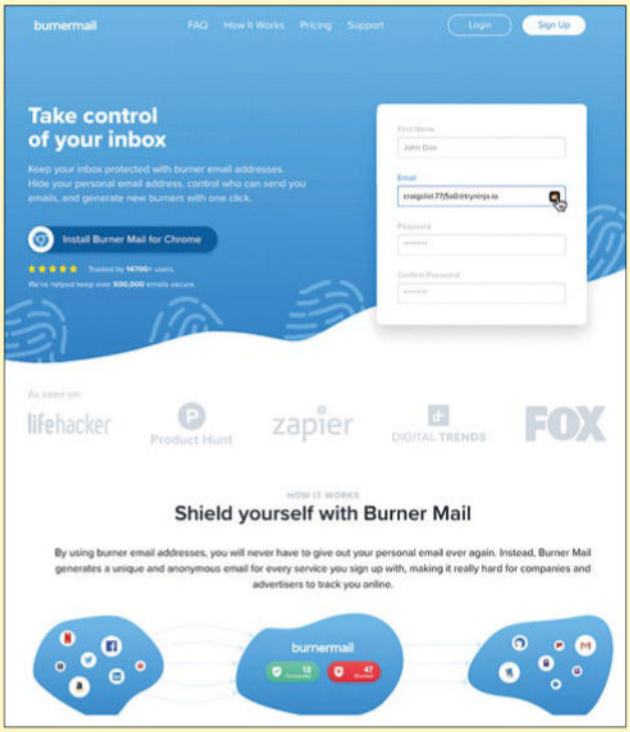
Fake Mail Generator, o Email Temporal Gratis en su versión en español, es una herramienta online que te permite crear direcciones de correo electrónico desechables en segundos. Este sitio web es muy fácil de usar y no requiere ningún tipo de registro, las direcciones generadas tiene una vigencia de 24 h y, transcurrido ese periodo, se eliminan junto a los emails recibidos. Puedes personalizar la dirección de correo e incluso seleccionar entre varios dominios disponibles, de diferentes países, por si el servicio al que quieres acceder tiene bloqueadas las direcciones de correo de tipo temporal. Los correos que recibas se mostrarán de inmediato en una bandeja accesible desde la misma página, sin necesidad de actualizarla manualmente. Se trata de una herramienta especialmente útil si necesitas verificar cuentas rápidamente o probar servicios sin comprometer tu correo real. Eso sí, al igual que otros servicios similares, no es recomendable usarlo para recibir información confidencial o que resulte especialmente importante para el usuario.

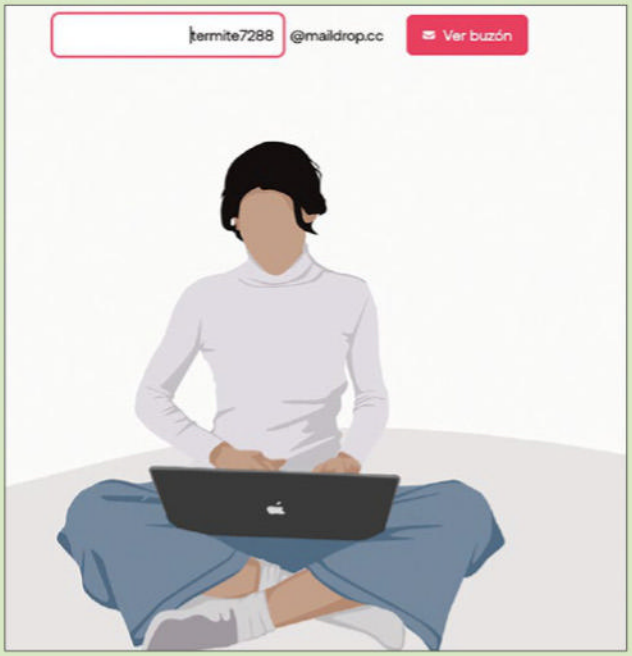
Página web: bit.ly/3TO3EhL

BURNER MAIL

Burner Mail es un servicio de correo temporal que requiere registro y ofrece opciones gratuitas y de pago. A diferencia de otras plataformas, permite crear direcciones falsas que reenvían mensajes a tu correo real sin revelar tu dirección personal. De esta forma, podrás bloquear remitentes de spam, saber qué sitios venden tus datos y eliminar direcciones filtradas. La versión gratuita incluye funciones básicas. Sin embargo, si pagas, podrás gestionar más direcciones y personalizalas mejor. Burner Mail protege tu privacidad con cifrado TLS, SPF, DKIM y almacena todo en servidores seguros de Amazon. Además, no guarda correos reenviados ni vende tus datos. Funciona con cualquier correo y permite responder sin mostrar tu identidad real.

Página web: burnermail.io





MAILDROP

MailDrop es una opción también muy práctica a la hora de crear un correo desechable y recibir mensajes sin revelar tu dirección personal. No requiere contraseña ni suscripción, y permite elegir un nombre personalizado para la dirección, lo que facilita recordarla o reutilizarla cuando sea necesario. Cada bandeja de entrada puede almacenar hasta 10 mensajes, pero si no recibe correos en 24 h, se vaciará automáticamente para de esta forma lograr liberar espacio. Además, MailDrop cuenta con un espacio limitado para todos los mensajes, por lo que las bandejas inactivas se eliminan para dar prioridad a las más activas. Esto ayuda a mantener el servicio ágil y funcional. También filtra automáticamente el spam, eliminando correos con archivos adjuntos o contenido peligroso, lo que lo hace ideal para registrarte en sitios poco fiables o evitar saturar tu bandeja principal. Para acceder a tu bandeja, solo debes introducir el nombre personalizado en la web de MailDrop, sin necesidad de registrarte ni iniciar sesión.

Página web: maildrop.cc

MAILINATOR

Mailinator permite crear direcciones de correo temporal que duran hasta 24 h, sin necesidad de registrarse. Solo tienes que elegir un nombre y podrás usarlo con el dominio ***@mailinator.com*** para recibir correos de forma anónima y rápida. Es ideal para proteger tu privacidad y evitar usar tu correo personal en sitios poco fiables o temporales. La plataforma ofrece opciones avanzadas de pago con funciones adicionales y mayor control, pero la versión gratuita funciona sin registro ni complicaciones. Así, podrás recibir mensajes temporales fácilmente y mantener tu bandeja principal limpia, segura y organizada.

Página web: www.mailinator.com

¿ESTÁN TUS DATOS PERSONALES EN LA DARK WEB?

Si quieres saber si tus datos han sido compartidos en alguna de las listas que se venden en la Dark Web, existen herramientas especializadas que evitan que los ciberatacantes puedan acceder a otros datos asociados.

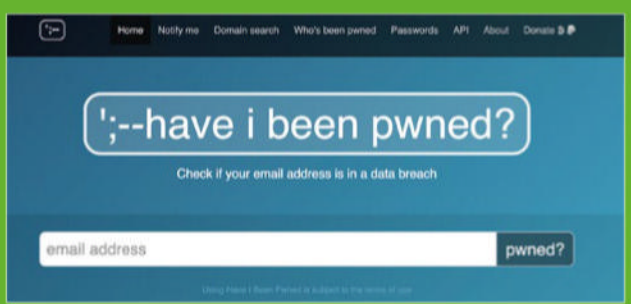
Descubrir que tu información personal se ha filtrado en la Dark Web nunca es una buena noticia. En estas listas con miles de **nombres, apellidos, direcciones** y, en el peor de los casos, **cuentas bancarias o información sensible**, los ciberdelicuentes siempre encuentran el material para llevar a cabo estafas. Aunque la filtración de datos como tu nombre o correo puede parecer menos peligrosa, siempre se recomienda cambiar tus contraseñas, activar la verificación en dos pasos y, para mayor seguridad, configurar códigos temporales. Estas medidas son la mejor defensa ante una filtración, ya que los atacantes suelen recurrir a la ingeniería social para elaborar un perfil detallado y hacerse pasar por un servicio legítimo, llenando tu bandeja de entrada con **correos fraudulentos o spam diseñados para engañarte**.

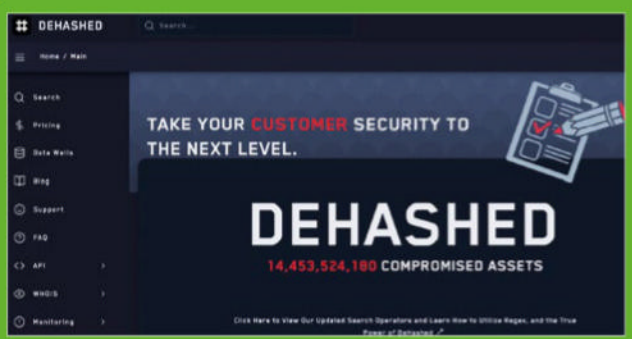
Si te preocupa tu seguridad, aquí tienes una lista con algunas de las mejores herramientas para averiguar si tus datos personales se han filtrado y conocer el estado de los ciberataques en todo el mundo.

HAVE I BEEN PWNED

Esta herramienta es, sin duda, una de las más populares para saber si tus datos están en la Dark Web. Además, es la primera que cualquier usuario debería visitar, si quiere saber si su correo electrónico forma parte de un directorio de datos personales expuesto tras una brecha de seguridad. Con solo introducir tu correo, el sitio te indicará si ha sido comprometido en alguna filtración masiva, detallando con claridad la empresa que sufrió el ataque y el tipo de datos comprometidos. Creada en el año 2013 por Troy Hunt, director regional de Microsoft y reconocido experto en ciberseguridad, esta herramienta ofrece una gran fiabilidad y precisión que la han hecho indispensable para millones de usuarios.

Página web: haveibeenpwned.com





DEHASHED

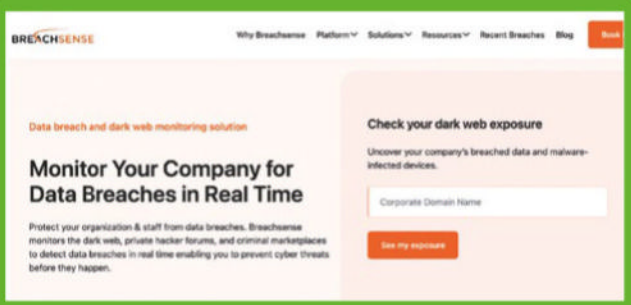
Se trata de una de las herramientas más completas de la lista, ya que no solo permite acceder a filtraciones de correos electrónicos, sino también a cualquier dato personal asociado contigo como tu nombre, apellidos, dirección IP, nombre de usuario o dirección postal, entre otros. Lo mejor de todo es que puedes acceder a esta información sin tener que pagar nada, ya que el servicio es gratuito al crear una cuenta nueva. Por todo esto, la recomendamos como una de las principales opciones, especialmente si sospechas que tus datos personales pueden estar comprometidos, ya que la versión gratuita ofrece una gran cantidad de funciones.

Página web: dehashed.com

SPYCLOUD

Este es uno de los servicios más populares, a la hora de comprobar si tus datos personales han sido filtrados. Y aunque está principalmente orientado a servicios empresariales o correos electrónicos corporativos, también está disponible para usuarios individuales. La versión gratuita de SpyCloud ofrece solo información básica como la fecha de la brecha, el nivel de riesgo asociado al ciberataque y los datos filtrados. Si deseas acceder a un informe más detallado, tendrás que optar por la versión Premium, que es de pago. En resumen, te recomendamos explorar primero otras herramientas, ya que algunas proporcionan un análisis más completo en su versión gratuita.

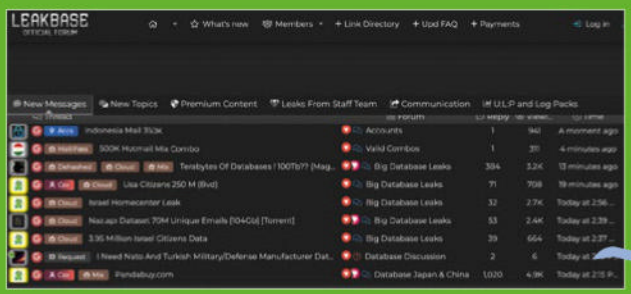
Página web: spycloud.com/es



BREACHSENSE

Es posible que la empresa para la que trabajas haya sido víctima de un ciberataque, lo que podría haber expuesto tus datos a los delincuentes de la Dark Web. Con BreachSense, podrás saber si el dominio de tu compañía ha sido afectado por una filtración masiva de datos o, en el peor de los casos, si las credenciales de acceso han quedado expuestas. A diferencia de otras plataformas, BreachSenno no se centra principalmente en la búsqueda de datos personales como tal, salvo el correo electrónico, ya que su enfoque se basa en revisar el dominio de un sitio web específico, identificando brechas de seguridad y posibles filtraciones relacionadas con el entorno corporativo y sus datos confidenciales.

Pagina web: www.breachsense.com



LEAKBASE

Aunque esta herramienta no funciona como un buscador de datos personales al uso, puede ser una buena opción si quieres conocer el estado general de las brechas de seguridad a nivel global en el mundo. Ofrece listados completos de los ciberataques más recientes, incluyendo detalles como la fecha de exposición y otros datos relacionados como inicios de sesión y contraseñas comprometidas. La plataforma funciona de manera similar al un foro tradicional, donde colaboradores y usuarios comparten información sobre nuevas filtraciones de información y su potencial venta en la Dark Web. Todo esto convierte a Leakbase en una opción realmente útil para quienes buscan mantenerse informados sobre el panorama general de la ciberseguridad y las amenazas emergentes.

Página web: leakbase.io

INTELLIGENCEX

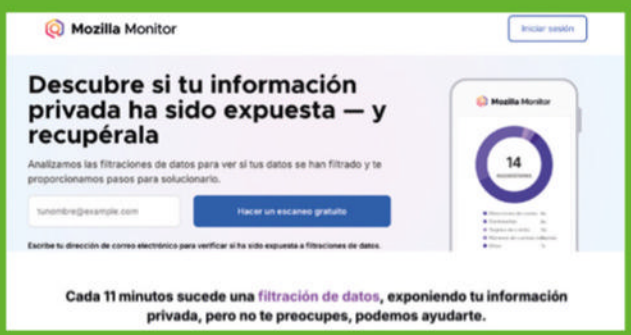
Esta herramienta también te permite buscar información sobre posibles filtraciones en la Dark Web. Aunque la creación de una cuenta en esta plataforma es gratuita, el acceso completo a información detallada sobre la brecha requiere una suscripción a la versión Pro. Esta opción de pago desbloquea datos más exhaustivos, como la fecha y hora exacta de las filtraciones, y también ofrece la posibilidad de descargar archivos txt con información sobre los datos filtrados. En cualquier caso, se trata de una herramienta útil para aquellos que desean investigar a fondo qué documentos han sido comprometidos y vendidos de forma ilicita, brindando más detalles que un simple aviso sobre las brechas de seguridad. En algunos casos, los resultado pueden coincidir perfectamente con eventos de filtraciones conocidas, ofreciendo así una visión mucho más precisa sobre la exposición de los correos y otra información personal.

Página web: intelx.io

MOZILLA MONITOR

Si hay algo en lo que ponga especial interés el navegador Mozilla Firefox es en la apuesta por la privacidad de los usuarios, así que no podía falta una herramienta propia para saber si tus datos han sido comprometidos. Antes conocida como Firefox Monitor, Mozilla Monitor permite saber si tu dirección de correo electrónico ha formado parte de alguna filtración masiva. Para saber si tus datos han sido robados por los hackers, lo único que tienes que hacer es acceder al sitio web de la plataforma e introducir tu dirección de correo en el campo de texto ***Enter Email Address***. Luego, haz clic en el botón ***Scan***. Transcurridos unos segundos, el sistema te mostrará en los resultados las veces que tu correo electrónico se ha visto comprometido en una brecha de seguridad y los datos que han caído en manos de los ciberdelincuentes. Para mayor tranquilidad, Firefox ofrece recomendaciones de seguridad para proteger tu información, que incluyen consejos sobre contraseñas fuertes, privacidad online y el modo de evitar sitios web peligrosos.

Página web: monitor.mozilla.org



IMÁGENES OCULTAS EN GOOGLE FOTOS

CARPETA PRIVADA

La función Carpeta privada lleva ya un tiempo formando parte de las opciones de la aplicación Fotos. Con ella, Google quiere aportar un plus de privacidad a todos los usuarios que lo necesiten.

Aprende a...

Utilizar la función 'Carpeta privada' desde la app Google Fotos de tu dispositivo móvil. Podrás así asegurar fácilmente la privacidad de tus fotos personales.

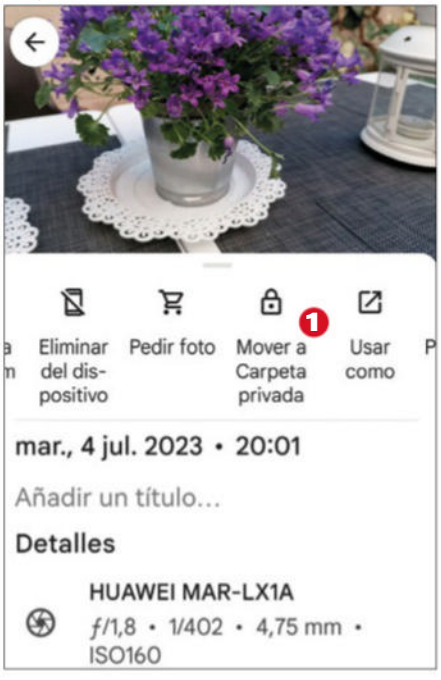
Esta herramienta para Google Fotos se desplegó, en un principio, solo para los usuarios con móviles Pixel. Sin embargo, su buena recepción desde el inicio hizo que fuera llegando de forma gradual al resto de dispositivos Android.

Se trata de una carpeta muy especial de Fotos te permite almacenar en ella una serie de fotografías de manera privada, para que no aparezcan en la vista principal de la app, en las búsquedas o, por ejemplo, en los álbumes de Fotos. ¡Incluso no serán accesibles por ninguna otra app! Además, para abrir la carpeta privada se requiere una autenticación adicional (un PIN o la huella dactilar), lo que la hace aún más segura. No obstante, debes tener presente que si borras la app Fotos de tu teléfono o cambias de dispositivo, perderás todas las imágenes que estén en esa carpeta privada.

1 Si quieres empezar a utilizar tu Carpeta privada desde Google Fotos, pulsa en el icono inferior ***Biblioteca*** y, a continuación, pulsa también en el denominado ***Utilidades***. Esto te dará acceso al apartado ***Configurar Carpeta Privada***. Elige ***Empezar***.

2 La aplicación te mostrará entonces, en una nueva pantalla, todas características de esta función, para que así puedas empezar a guardar fotografías en ella. Pulsa en ***Configurar***, accede con tu PIN o huella dactilar y empieza a incluir fotos en esta carpeta. Hazlo con clics en ***Mover elementos***. Como verás, los detalles son los que te hemos comentado, pero no podemos mostrártelos aquí por un motivo lógico: esta función no nos deja hacer capturas de pantalla. ¡Ante todo es una apuesta de Google por la privacidad!

3 Otra manera de añadir fotos a esta carpeta en cualquier momento consiste en localizar la imagen en cuestión del modo habitual. Seguidamente, con la foto ya en pantalla, arrastra hacia arriba para acceder a sus propiedades y, en esta ocasión, elige la entrada ***Mover a Carpeta privada*** (1). Sigue luego con una pulsación sobre ***Continuar***.



CONSEJOS PARA MEJORAR EL CONTROL PARENTAL

¿Sabes lo que hace tu hijo en Internet? Aquí tienes los mejores trucos para ejercer un mayor control parental en el ordenador y en el móvil.

Ciberacoso, conversaciones con personas un tanto sospechosas, imágenes violentas y **contenidos perjudiciales para los menores**: si Internet se usa sin filtros, es cualquier cosa menos un lugar seguro para los niños. Si quieres proteger a tus hijos de estos peligros, lo primero que tienes que hacer es: ¡instruirlos al respecto! Pero por mucha disposición que tengan hacia el diálogo, a menudo con los pequeños se aplica también una premisa: la confianza está bien, pero el control es mucho mejor.

Ordenador y teléfono móvil adecuados para niños

Google ofrece una buena solución con la que puedes controlar y dirigir el uso del móvil por parte de tus hijos, que además es gratuita. De esta forma, podrás determinar **cuánto tiempo al día pueden pasar tus hijos en Internet**, qué páginas pueden visitar y, en caso necesario, saber dónde se encuentran en un determinado momento, entre otras cosas. Asimismo, existen otras opciones de supervisión, por ejemplo, el software de control parental de Salfeld que puedes descargar para el ordenador desde la página web del fabricante (**salfeld.com/en/download**) o desde la tienda de aplicaciones de Android (consulta la columna del borde derecho de la página derecha) o un reloj inteligente (smartwatch) para niños, que te mantiene informado en todo momento del paradero de tu hijo en la vida real. Ejemplos de relojes inteligentes son el SaveFamily o el Xplora X5 Play. Este último, por ejemplo, **cuenta con GPS y un sistema de área de seguridad**. También permite enviar mensajes de voz, de texto y emojis.

Con estos recursos a tu alcance, te asegurarás de que tu hijo se maneje en su vida digital de una forma sana y segura.

1 INSTALACIÓN EN LOS MÓVILES ANDROID GOOGLE FAMILY LINK

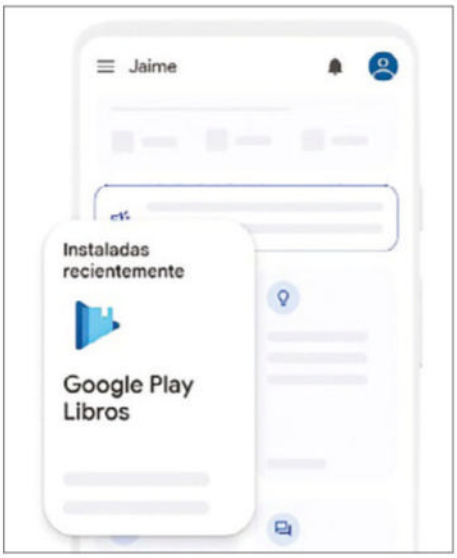
ANDROID

Google Family Link es una aplicación que te permitirá saber en todo momento cómo usan tus hijos los móviles que están equipados con el sistema operativo Android. Así funciona:

1 Lo que debes saber para comenzar: como progenitor, puedes utilizar Google Family Link en tu iPhone o en tu móvil Android, pero tu hijo tiene que tener, sí o sí, un Android. Algo que también es importante: tanto tú como tu hijo necesitáis una cuenta en Google. Por tanto, créalas en **www.google.com**.

2 Instala luego en tu móvil la aplicación Google Family Link desde la Play Store de Google o desde la App Store de Apple. Ábrela, inicia sesión con tu cuenta de Google y prepara el dispositivo de tu hijo. Para ello, ve a ***Ajustes*** en el teléfono de tu hijo y sigue los pasos que se te muestran en la aplicación, para de esta forma poder vincular la cuenta de tu hijo con la tuya.

3 Una vez que tu cuenta se encuentre vinculada con la de tu hijo, tendrás que pulsar en ***Permitir*** para dar acceso al control parental. A continuación, podrás seleccionar las aplicaciones y opciones que consideres adecuadas para gestionar con detalle cómo quieres que tu hijo use el móvil desde ese momento.



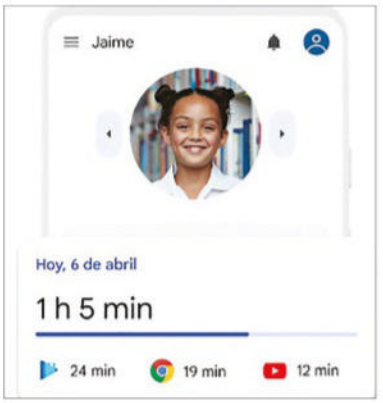
Solo contenidos adecuados: gracias a Family Link, puedes orientar a tu hijo sobre qué aplicaciones debería utilizar.

ANDROID

2 COMO PROGENITOR, UTILIZA **FUNCIONES DE PROTECCIÓN**

Si has configurado Family Link en el móvil, la aplicación te ofrece algunas funciones para proteger a tu hijo, por ejemplo:

- **Establece límites de tiempo:** toca en el perfil de tu hijo. A continuación, en ***Controles*** y ***Límite diario***. Ahí puedes establecer cuánto tiempo al día puede navegar tu hijo por Internet y cuánto tiempo puede usar cada aplicación.
- **Comprueba dónde está tu hijo:** ¿te preguntas dónde se encuentra en este momento tu hijo? Family Link te lo muestra, por defecto, directamente bajo el perfil correspondiente. También se pueden asignar etiquetas a determinados lugares. Para ello, en ***Ubicaciones***, ***Lugares de familia*** y ***Nuevo lugar***, añade la dirección que corresponda y ponle también un nombre en el cuadro de texto ***Etiqueta de ubicación***.
- **Gestiona el comportamiento de uso:** en el perfil de tu hijo, Family Link te muestra las aplicaciones que acaba de usar el menor y todas las nuevas aplicaciones que ha instalado.



ANDROID

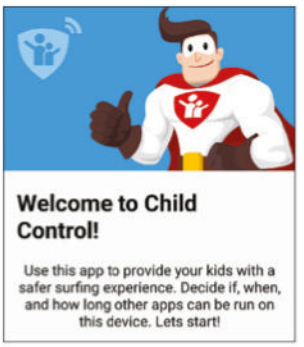
Con la app Family Link, mantienes el control de las aplicaciones que se instalan en el teléfono móvil.

3 CUANDO LOS HIJOS **PIDEN MÁS**

Tu hijo podrá usar el móvil conforme a las indicaciones que hayas establecido en el paso anterior. Si quiere algo más, tendrá que pedirlo.

- **Más tiempo:** por ejemplo, si has establecido un límite para el uso de YouTube, un par de minutos antes de llegar a ese límite, se recibe un aviso. Una vez que se llega al límite, la aplicación se cierra y no se puede volver a abrir hasta el día siguiente. ¿Te pide tu hijo más tiempo y quieres permitírselo? Entonces, abre Family Link, toca en la pantalla de inicio en el nombre de tu hijo y selecciona ***Controles*** y ***Límites de aplicaciones***. A continuación, toca el pequeño reloj de arena que aparece junto a YouTube y elige ***Cambiar el límite de la aplicación***. Establece el nuevo límite y cierra la aplicación con ***Hecho***.
- **Nuevas aplicaciones:** si al configurar el control parental has seguido las directrices recomendadas, tu hijo no podrá instalar por sí mismo nuevas aplicaciones. Si lo intenta, se le mostrará un aviso en ese momento. Si te envía un mensaje para que apruebes la instalación, recibirás tú también un aviso sobre ello.

PARA MÓVIL Y ORDENADOR: SALFELD



¿Demasiado tiempo en Internet? Con el control parental de Salfeld, podrás establecer límites de tiempo y también de uso.

Mediante Family Link, solo podías supervisar móviles Android. Para iPhone o iPad, no funciona la aplicación. Si quieres mantenerte informado del uso de un móvil o tablet de Apple o de un ordenador, puedes utilizar la aplicación de control parental de Salfeld (solo en inglés o alemán). Descárgala desde la página web del fabricante (**salfeld.com/en/download**) o desde la tienda de aplicaciones de tu móvil. La aplicación puede probarse durante un mes gratis, después hay que pagar. Desde el portal de Salfeld, puedes mantenerte al tanto del comportamiento de uso de tu hijo en los dispositivos compatibles. Al igual que ocurre en Family Link, puedes establecer límites temporales para los dispositivos y las aplicaciones o bloquear las que tú determines. También puedes localizar el dispositivo móvil y obtener informes sobre cómo lo está usando tu hijo.

Con los filtros web, puedes determinar el tipo de páginas web que tu hijo podrá visitar o, si lo ves necesario, también darle acceso libre a todos los contenidos.

¡INCLUSO ANTES DE ABRIRLO!

CÓMO COMPROBAR SI UN ARCHIVO DE INTERNET ES SEGURO

Antes de abrir cualquier fichero o documento, conviene comprobar que es seguro y así evitar malware, virus, troyanos o ransomware. Existen varias formas sencillas de hacerlo en Windows.

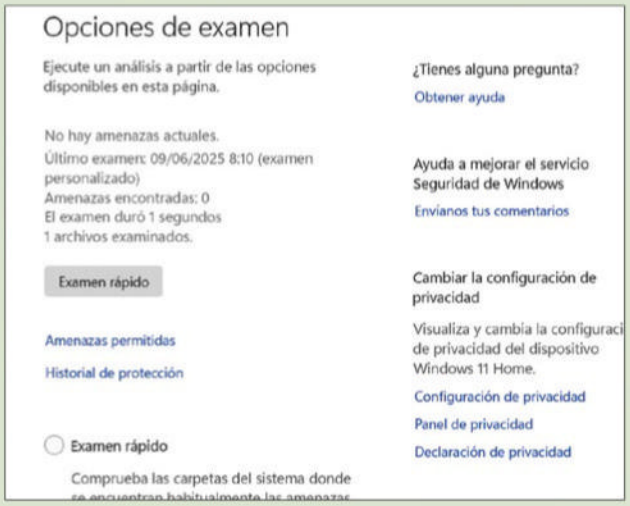
Descargar archivos de Internet se ha vuelto una acción tan cotidiana que muchos lo hacen **sin pensarlo dos veces**: un documento del trabajo, una imagen enviada por un amigo, una herramienta gratuita para editar vídeos o incluso una actualización de software que no aparece en el sitio oficial.

Sin embargo, lo que puede parecer una acción habitual puede convertirse en **una de las mayores amenazas** informáticas: descargar malware camuflado que contiene código malicioso capaz de acceder a tus datos e información personal.

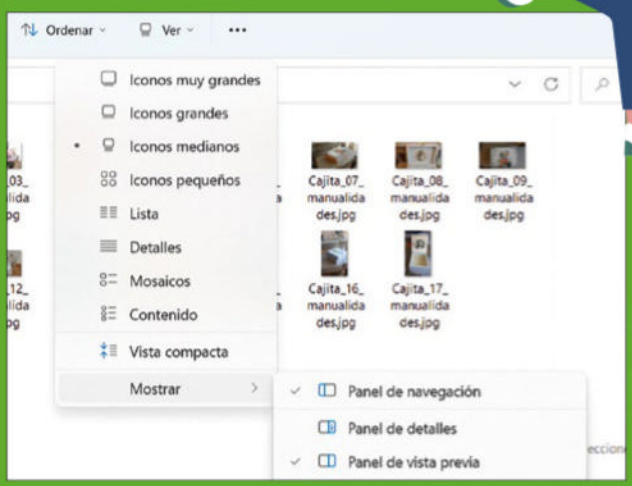
Tener un **antivirus instalado** es clave para proteger tu equipo, pero si no cuentas con uno, aquí te mostramos seis formas de comprobar si un archivo es seguro antes de abrirlo en tu ordenador con Windows.

ANALÍZALO CON LA **HERRAMIENTA DE SEGURIDAD** DE WINDOWS

Tu ordenador con Windows ya incluye un sistema de protección que puedes usar en cualquier momento. Para utilizarlo, basta con hacer clic con el botón derecho del ratón sobre el archivo que has descargado y seleccionar la opción ***Examinar con Microsoft Defender***. En la nueva ventana, podrás elegir ***Examen rápido***. Esta es una herramienta discreta, pero bastante eficaz y capaz de detectar numerosas amenazas habituales. Además, no requiere ninguna configuración adicional ni poseer conocimientos avanzados. En unos segundos, te dirá si detecta algo sospechoso.



Examinar con Microsoft Defender permite detectar amenazas ocultas en archivos y carpetas, ofreciendo una protección rápida y eficaz.



Mostrar las extensiones de archivo facilita identificar formatos y aumenta la seguridad al evitar abrir archivos maliciosos accidentalmente.

COMPRUEBA LAS **EXTENSIONES** DE LOS ARCHIVOS

Una de las trampas más antiguas, pero que aún funciona, consiste en cambiar el nombre de los archivos para que parezcan otra cosa. Un fichero que dice ser un ***documento.pdf*** puede ser en realidad ***documento.pdf.exe***, y si no tienes activada la opción para visualizar las extensiones, no te percatarás del engaño. Para evitarlo, accede a las opciones del Explorador de archivos: desde la barra de menús superior, elige ***Ver***, ***Mostrar*** y ***Extensiones de nombre de archivo***. Así sabrás siempre si estás a punto de abrir una imagen, un documento real o algo que puede ejecutar código malicioso sin que lo sepas.

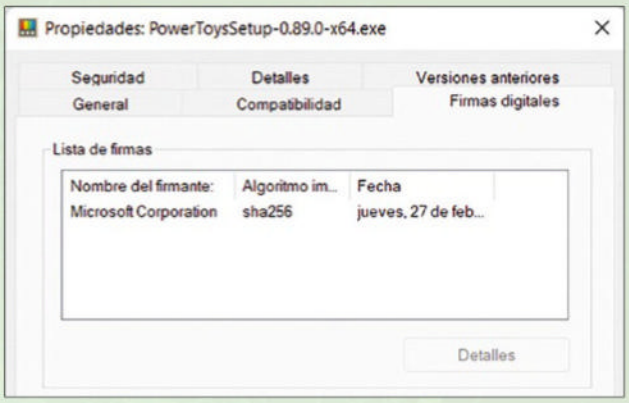
VirusTotal analiza archivos y enlaces con múltiples antivirus simultáneamente, detectando amenazas que un solo programa podría pasar por alto.

ES POSIBLE RECURRIR A **HERRAMIENTAS ONLINE**

Si tienes dudas sobre un archivo, puedes recurrir a herramientas gratuitas online como VirusTotal (**www.virustotal.com**). Este sitio web permite subir archivos sospechosos para que sean analizados por más de 70 motores antivirus. Si varios de ellos detectan algo inusual, lo más prudente es no abrirlo. No necesitas instalar nada ni crear una cuenta, lo que lo convierte en una opción muy útil cuando recibes un archivo por correo electrónico o por servicios de mensajería y no estás seguro de su procedencia.

VERIFICA SI EL ARCHIVO TIENE UNA **FIRMA DIGITAL**

Los programas legítimos suelen incluir una firma digital que certifica su autenticidad y garantiza que no han sido modificados. Para comprobarlo, haz clic derecho sobre el archivo de la aplicación, selecciona ***Propiedades*** y la pestaña ***Firmas digitales***. Si ves el nombre del desarrollador y todo está correctamente firmado, es una buena señal. En cambio, si no hay firma o el emisor te resulta desconocido, es recomendable desconfiar. Esta verificación es especialmente útil cuando descargas software desde páginas poco conocidas, ya que te ayuda a detectar posibles alteraciones maliciosas.



Verificar la firma digital en las propiedades del archivo garantiza su autenticidad y asegura que no ha sido modificado ni manipulado.

VirtualBox permite crear máquinas virtuales para probar software, sin afectar el funcionamiento del sistema principal del equipo.

ÁBRELO EN UN **ENTORNO AISLADO**

Si usas Windows 10 u 11 Pro, puedes aprovechar Windows Sandbox, una función que permite ejecutar archivos en un entorno aislado, similar a un escritorio virtual. De este modo, si el archivo contiene código malicioso, los posibles daños no afectarán a tu sistema principal. Como alternativa, también puedes utilizar máquinas virtuales gratuitas como VirtualBox (**www.virtualbox.org**) para lograr el mismo efecto. Esta es una solución especialmente útil cuando necesitas abrir un archivo pero no confías completamente en su origen, ya que todo queda contenido dentro de un entorno cerrado que puedes eliminar sin dejar rastro.

NO IGNORES NUNCA LAS ADVERTENCIAS DE SEGURIDAD DE **SMARTSCREEN**

Cuando haces doble clic en un archivo descargado y aparece una advertencia, se trata de SmartScreen, el filtro de seguridad de Microsoft. Esta herramienta analiza el archivo según su reputación: si es común y ha sido abierto sin problemas por muchos usuarios, lo permitirá; pero si es nuevo, poco habitual o potencialmente peligroso, te avisará. Aunque algunos usuarios lo desactivan por considerarlo molesto, SmartScreen es una de las capas de defensa más eficaces en Windows. Si aparece una advertencia, no la ignores: tómala como una oportunidad para revisar el archivo, investigar su origen y aplicar cualquiera de las comprobaciones anteriores antes de ejecutarlo. Para asegurarte de que SmartScreen está activado, ve al menú Inicio, escribe ***Seguridad de Windows***, accede a ***Control de aplicaciones y navegador*** y, en ***Configuración de protección basada en reputación***, asegúrate de que la función esté activada.

SmartScreen protege bloqueando archivos y avisando antes de abrirlos.

KIOSKEROS

LO MEJOR CONTRA LOS

10
SOLUCIONES
ANTIVIRUS

VIRUS 2025

Las tradiciones son así: vuelve a ser el momento de comprobar cuál es la mejor y más que necesaria protección antivirus de este año.

La peligrosidad de Internet para los particulares aumenta sin cesar. No solo es cada vez más fácil para los delincuentes **crear malware sin conocimientos de programación**, también hay cada vez más estafas de phishing y fraude. Kaspersky observó cientos de millones de ataques de phishing en Europa en 2024 y es probable que el número de casos no denunciados sea significativamente mayor. Esto hace que sea aún más importante protegerse con un paquete de seguridad fiable. De ahí que pongamos a prueba los diez programas antivirus más importantes, junto a algunos consejos a tener en cuenta a la hora de comprarlos.

Conjuntos todoterreno

Un antivirus por sí solo ya no basta para responder a las diversas amenazas actuales. De ahí que se prueben los paquetes completos de cada fabricante, con los que realmente parecen hacer un gran esfuerzo por maximizar la seguridad. Los paquetes incluyen funciones como VPN, gestor de contraseñas, protección de la identidad y mucho más. Los expertos han comprobado cuidadosamente las diferencias entre proveedores, por lo que merece la pena prestar atención a cada apartado.

La mejor protección

Todos los programas probados ofrecen una protección antivirus buena o, incluso, muy buena. Esto significa que, con cualquiera de los candidatos de la prueba correctamente instalado y actualizado, no hay que preocuparse demasiado por la entrada de malware en el PC.

PROTECCIÓN PARA **ARM**

Algunos dispositivos actuales trabajan con un procesador ARM, como los Snapdragon. Los programas antivirus solo funcionan con ellos si el fabricante los ha adaptado para su uso. Este es el caso de muchos de ellos, pero no de todos. En la siguiente tabla, se puede ver si los candidatos a la prueba funcionan en dispositivos ARM. En caso de dudas sobre si se usa un dispositivo ARM, lo mejor es pulsar la tecla de ⊞, escribir ***Configuración*** y hacer clic en ***Configuración e información***. Si después de ***Tipo de sistema*** pone ***Procesador basado en ARM***, se trata de un dispositivo ARM.

Producto	Compatibilidad
NORTON 360 ADVANCED	✔
AVIRA PRIME	A partir de 2T 2025
BITDEFENDER ULTIMATE SECURITY	✔
MCAFEE+ ULTIMATE	✔
AVAST ONE GOLD	✔
KASPERSKY PREMIUM	✘
G DATA TOTAL SECURITY	A partir de 2026
F-SECURE TOTAL	✘
ESET HOME SECURITY ULTIMATE	✔
MICROSOFT DEFENDER	✔

Sin embargo, hay grandes diferencias en los detalles. Avira Prime, por ejemplo, reconoció el 99,955 % del malware en la prueba de laboratorio y lo bloqueó todo. Con Microsoft Defender, la cifra baja al 99,891 %. Sin conexión a Internet, cuatro programas suspenden: Norton, McAfee, Kaspersky y Microsoft Defender. Mientras que Bitdefender y G Data siguen bloqueando más del 95 %. Por tanto, merece bastante la pena echar un vistazo a la tabla completa de las siguientes páginas antes de adquirir un software.

Norton vuelve a ganar ahora

Norton 360 Advanced defiende su trono del año pasado y vuelve a ser el ganador del conjunto del test. Sin embargo, la competencia de Avira y Bitdefender apenas es peor. Norton se impuso porque, además de una buena protección antivirus y excelentes funciones, es el único programa con una buena valoración de los usuarios. No solo ofrece una protección fiable, sino que también es rápido y realmente fácil de usar.

Con Norton, ganador de la prueba, se ven las funciones más importantes en primer plano y el resto está a la izquierda, en las secciones correspondientes.

MS Defender baja el ritmo

Microsoft Defender, que viene **gratis con Windows**, sigue ofreciendo una buena protección contra el malware y recibe una calificación global satisfactoria. No está nada mal para una protección básica y virtualmente gratuita. Sin embargo, falla sin conexión a Internet y no tiene mucho que ofrecer contra los ataques de phishing. Por tanto, confiar en la protección de Windows a diario puede salir más caro que comprar un buen programa de protección. La realidad es que conviene sustituir el software de Microsoft por cualquier otro del banco de pruebas cuanto antes.

A Avast le sienta mal el test

Otra novedad positiva a destacar es que muchos fabricantes han mejorado sus **términos y condiciones** o sus políticas de privacidad. Los de G Data y la política de privacidad de ESET obtienen esta vez valoraciones muy buenas. Avast es una ex-

EL **COSTE** DE LA PROTECCIÓN ANTIVIRUS

Los precios de los programas antivirus pueden confundir. No solo los fabricantes cobran cantidades diferentes entre sí, sino que los paquetes también contienen distintos números de licencias. A continuación, hay un resumen de los más habituales para no tener que buscar y calcular en cada uno de los sitios web de los fabricantes. No importa cuántas licencias hacen falta en casa o la oficina, merece la pena comparar para así poder ahorrar dinero y usarlo de otra manera mejor.

Producto	Precio por 1 licencia	Precio por 5 licencias	Precio por 10 licencias	Precio por 20 licencias
NORTON 360 ADVANCED	44,99 €	44,99 €	44,99 €	89,98 €
AVIRA PRIME	59,95 €	59,95 €	119,90 €	134,95 €
BITDEFENDER ULTIMATE SECURITY	79,99 €	79,99 €	109,99 €	109,99 €
MCAFEE+ ULTIMATE	104,95 €	114,95 €	114,95 €	114,95 €
AVAST ONE GOLD	39,48 €	39,48 €	62,28 €	124,56 €
KASPERSKY PREMIUM	34,99 €	42,99 €	59,99 €	67,99 €
G DATA TOTAL SECURITY	49,95 €	81,95 €	163,90 €	327,80 €
F-SECURE TOTAL	69,99 €	99,99 €	199,98 €	399,96 €
ESET HOME SECURITY ULTIMATE	119,99 €	119,99 €	144,99 €	289,98 €
MICROSOFT DEFENDER	Gratuito	Gratuito	Gratuito	Gratuito

cepción. No solo sigue conteniendo muchas cláusulas inválidas o desfavorables, sino que ahora el fabricante incluso prohíbe las pruebas sin su consentimiento. Hasta ahora, este solía ser el caso de los programas dudosos que quieren evitar que el usuario final descubra sus puntos flojos. A pesar de las trabas, los resultados están en estas páginas. Curiosamente, Avast sale bien parado y no tiene sentido que hagan cosas de este tipo.

Una laboriosa tarea

La protección de todo lo que contiene un equipo informático es un tema muy importante. Es por esto que las pruebas se hacen junto con el renombrado laboratorio **AV-Comparatives** y **esb Rechtsanwälte**. Solo así es posible garantizar que los resultados de las pruebas son realmente significativos y que se puede confiar en ellos.

¿Portátiles sin protección?

Algunos portátiles nuevos tienen los llamados procesadores ARM. Son especialmente eficientes desde el punto de vista energético, y están optimizados para Copilot, la IA de Microsoft. Como comprador, no siempre se sabe que estos procesadores funcionan sin problemas con Windows, pero algunos programas tienen que adaptarse. Esto incluye también a los antivirus. Por desgracia, no todos los candidatos de la comparativa funcionan con **Windows basado en ARM**. En el recuadro de la página anterior se puede comprobar qué dispositivos tienen un procesador de este tipo y qué programas funcionan ya o lo harán con él.

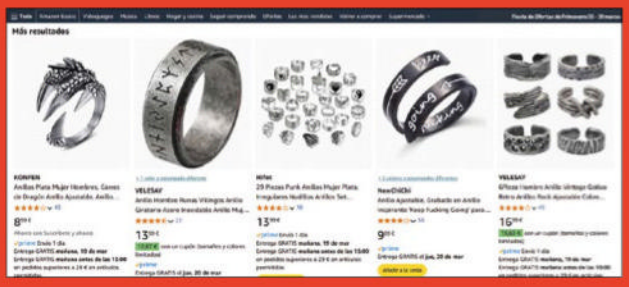
Anonimato sin terceros

Algunos candidatos a las pruebas también ofrecen **VPN o funciones de optimización**. Con las VPN, el objetivo es la protección en redes inseguras. Se trata de un complemento útil en paquetes de seguridad, pero los programas de terceros son más adecuados para reproducciones en streaming y juegos, aunque últimamente estos acostumbran a penalizar su uso. En cuanto a la optimización, los paquetes de protección suelen ofrecer menos que los programas especializados, así que es mejor comprobar lo que traen y si es más apropiado usar un software dedicado a afinar el sistema.

CONCLUSIÓN

El campo de pruebas en el sector antivirus está cada vez más apretado. Apenas hay distancia entre el primero y el noveno clasificado. Se nota el alto nivel en las puntuaciones, y todos los programas en el top nueve hacen su trabajo con fiabilidad. Norton ocupa el primer puesto y sigue siendo un poco mejor que la competencia. Microsoft Defender queda ligeramente rezagado en el último puesto y no puede seguir el ritmo de las nuevas amenazas. Sin embargo, la prueba también demuestra que es importante prestar atención antes de comprar, para así ahorrar y evitar chascos.

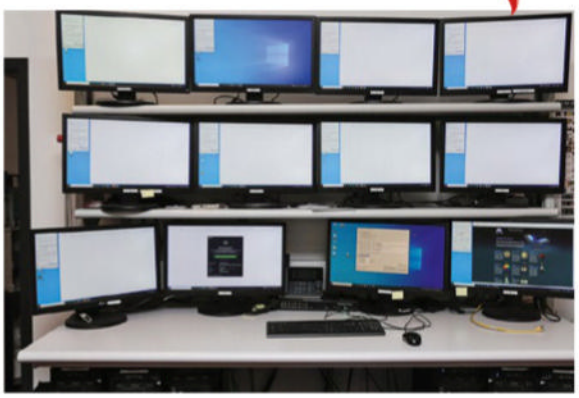
PROTECCIÓN CONTRA TIENDAS FALSAS



Las tiendas falsas son comercios online fraudulentos que a menudo ofrecen moda, tecnología, entradas para conciertos y mucho más a precios ventajosos... pero luego no entregan la mercancía. Detrás de ellas, hay delincuentes que simplemente quieren robar dinero. Como este tipo de tiendas aparecen cada vez con más frecuencia en Internet y apenas pueden distinguirse de las ofertas legítimas, los programas de protección deben advertir al entrar en un comercio falso.
Se ha incluido este punto en la tabla de la prueba de este año. El ganador de la prueba, Norton 360 Advanced, y McAfee+ Ultimate obtuvieron los mejores resultados aquí, ambos con una puntuación de Bien. Bitdefender Ultimate Security, G Data Total Security, Kaspersky Premium y Microsoft Defender, en cambio, tienen que ponerse al día. Todos han obtenido una puntuación de Insuficiente o Muy deficiente. Para evitar caer en la trampa de las tiendas falsas, antes de comprar en comercios online por primera vez, conviene comprobar algunas cosas, como el aviso legal y asegurarse de que el sitio no tiene advertencias negativas en el Centro de Asesoramiento al Consumidor de la comunidad autónoma, a nivel estatal o internacional.

BANCO DE **PRUEBAS** DE COMPUTER HOY

Un programa antivirus es el software más importante del PC. Si falla, puede costar dinero o mucho tiempo y nervios. Para probarlos con garantía, Computer Hoy colabora con el prestigioso laboratorio AV-Comparatives. Todos los candidatos a la prueba tienen que detectar, bloquear y eliminar correctamente un total de 20.131 entidades peligrosas en el laboratorio durante varios meses. También tienen que demostrar su capacidad durante este periodo en 960 sitios web reales infectados. Sin embargo, los programas no deben ser demasiado entusiastas y producir falsas alarmas. Al fin y al cabo, nadie quiere que se bloqueen y eliminen contenidos inofensivos. Además, AV-Comparatives comprueba hasta qué punto los programas ralentizan el trabajo diario. A nivel local, en su propio laboratorio, Computer Hoy comprueba la gama de funciones y lo intuitivos o fáciles de entender que son los programas. En definitiva, los usuarios también deben comprender lo que hay que hacer en caso de problemas. Ulrich Emmert, de esb Rechtsanwälte, examinó las condiciones legales y las disposiciones sobre protección de datos en nombre de la revista.



Los programas antivirus se ejecutan simultáneamente en un ordenador cada uno. Esto permite a los encargados compararlos con precisión y, además, evaluarlos de forma justa.

LA PRUEBA EN DETALLE

Efectividad, utilidades, efectos sobre el uso diario del ordenador o la facilidad de manejo son vitales para determinar cuál es el mejor de estos 10 productos probados por Computer Hoy.

1 NORTON 360 ADVANCED

Precio: 44,99 €
Otras versiones: 19,99 €

Disponibilidad: Windows, macOS, Android e iOS

Norton ha vuelto a salir victorioso y ha demostrado que es el mejor paquete del mercado. Con una protección antivirus muy buena y el manejo más sencillo en el campo de pruebas, está un paso por delante de la competencia. El único punto criticable: sin conexión a Internet, la tasa de detección baja demasiado, cosa que otros hacen mejor.

- + Manejo, protección antivirus, características variadas.
- − Si no cuenta con conexión a Internet, ofrece poca protección.

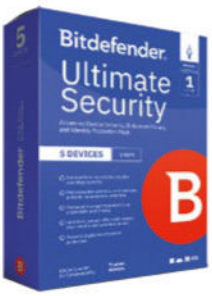
2 AVIRA PRIME

Precio: 59,95 €
Otras versiones: Gratuito

Disponibilidad: Windows, macOS, Android e iOS

Avira se mantiene a la altura del ganador de la prueba e, incluso, es un poco mejor en protección antivirus, ya que aguanta a buen nivel incluso sin Internet. Además, dispone de excelentes funciones. Sin embargo, Norton está por delante en cuanto a facilidad de uso. Pero Avira no es realmente malo en nada y, por tanto, merece el segundo puesto.

- + La mejor protección antivirus de la prueba, buenas funciones.
- − Algo complicado, sin protección infantil.



3 BITDEFENDER ULTIMATE SECURITY

Precio: 79,99 €
Otras versiones: Gratuito

Disponibilidad: Windows, macOS, Android e iOS

Bitdefender empata a puntos con el segundo clasificado, Avira, principalmente gracias a su excelente detección de malware y a sus funciones. Solo el manejo del programa es a veces engorroso, por ejemplo si se quiere desactivar el software de manera temporal. En general, Ultimate Security es un programa antivirus de primera.

- + Buena protección antivirus, grandes prestaciones.
- − Manejo complicado.

4 MCAFEE MCAFEE+ ULTIMATE

Precio: 114,95 €
Otras versiones: 29,95 €

Disponibilidad: Windows, macOS, Android e iOS

McAfee impresiona con una muy buena detección de malware en el laboratorio y en webs infectadas. Sin embargo, comete dos errores: la tasa de detección sin conexión a Internet es del 63,56 %. Esto es bajo y es el peor resultado de la prueba. Además, el software ofrece información limitada, pocas opciones de configuración y escasa comodidad.

- + Muy buena protección antivirus, mínima ralentización.
- − Peor protección sin Internet, complicado.

5 AVAST ONE GOLD

Precio: 39,48 €
Otras versiones: Gratuito

Disponibilidad: Windows, macOS, Android e iOS

Avast ofrece la mejor protección antivirus en el campo de pruebas junto a Avira. Sin embargo, los términos, las condiciones y las disposiciones de protección de datos son extremadamente pobres. No solo son a menudo inválidas, sino desfavorables para el usuario. Por ejemplo, el coste del precio de renovación se cobra 35 días antes.

- + Muy buena protección antivirus.
- − Condiciones generales y protección de datos inadecuadas.

	1 NORTON 360 ADVANCED	2 AVIRA PRIME	3 BITDEFENDER ULTIMATE SECURITY	4 MCAFEE MCAFEE+ ULTIMATE	5 AVAST ONE GOLD
PROTECCIÓN ANTIVIRUS					
	Muy buena detección de malware en el laboratorio, incluso en sitios infectados, muchos falsos positivos, mala protección sin Internet **9,00**	Muy buena detección de malware en la prueba de laboratorio, incluso en sitios infectados, pocos falsos positivos **9,20**	Muy buena detección de malware en el laboratorio, incluso en sitios infectados, pocos falsos positivos **9,00**	Muy buena detección de malware en el laboratorio, incluso en sitios infectados, algunos falsos positivos **9,00**	Muy buena detección de malware en el laboratorio, incluso en sitios infectados, pocos falsos positivos **9,20**
FUNCIONES					
	Cortafuegos, VPN, control parental, asistente de actualizaciones, copia de seguridad, eliminador de rastros, gestor de contraseñas **8,00**	Cortafuegos, VPN, escáner de vulnerabilidades, asistente de actualizaciones, gestor de contraseñas **7,20**	Cortafuegos, VPN, control parental, escáner de vulnerabilidades, protección antirrobo, asistente de actualizaciones, gestor de contraseñas **8,80**	Cortafuegos, VPN, eliminador de rastros, gestor de contraseñas **6,00**	Cortafuegos, VPN, escáner de vulnerabilidades, asistente de actualizaciones, eliminador de rastros **6,40**
RALENTIZACIÓN DEL PC					
	Inapreciable **9,20**	Apenas apreciable **8,80**	Apenas apreciable **8,80**	Inapreciable **9,80**	Inapreciable **9,20**
MANEJO					
	Mejor servicio, buenas condiciones generales y protección de datos **7,80**	Manejo algo complicado, buenas condiciones y protección de datos **6,80**	Manejo complicado, buena protección de datos **5,80**	Manejo más complicado, buena protección de datos **5,20**	Manejo complicado, deficientes condiciones generales y protección de datos **4,20**
Notable	**8,80**	**8,60**	**8,60**	**8,40**	**8,20**
Precio	**44,99 €**	**59,95 €**	**79,99 €**	**114,95 €**	**39,48 €**

COMPUTER HOY RESPONDE:

¿Cuál es el mayor peligro?

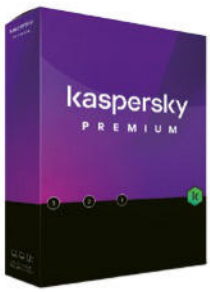
El phishing y el fraude que no para de actualizarse son actualmente la mayor amenaza para los particulares. Los delincuentes utilizan trucos psicológicos para robar dinero y datos. Encima, la protección contra ellos es limitada.

¿Qué es la protección de la identidad?

Si los delincuentes captan suficientes datos, pueden hacerse pasar por alguien y pedir préstamos, por ejemplo. La protección de identidad ayuda a encontrar estos datos y protegerlos. Además, avisa si existe una amenaza.

¿Por qué resultan tan peligrosos los deepfakes?

Los deepfakes son vídeos de personas generados por inteligencia artificial. Imitan a la perfección su aspecto y voz, de modo que a menudo es imposible distinguir la falsificación de la persona real. Esto permite perpetrar muchas estafas en las que los delincuentes se hacen pasar por la madre o el jefe de alguien, por ejemplo. Los hackers obtienen de esta forma información confidencial y pueden causar gastos o crear imágenes de desnudos y chantajear.



6 KASPERSKY PREMIUM

Precio: 42,99 €
Otras versiones: Gratuito

Disponibilidad: Windows, macOS, Android e iOS

Kaspersky sigue siendo objeto de una advertencia de la oficina de seguridad de la información, debido al riesgo de espionaje por parte de Rusia. Aparte de eso, Kaspersky ofrece las mejores funciones de la prueba y una buena protección antivirus. La protección de datos es insuficiente porque Rusia tiene acceso sin restricciones.

- + El mejor equipamento, buena protección antivirus.
- − Manejo complicado, protección de datos inadecuada.

7 G DATA TOTAL SECURITY

Precio: 81,95 €
Otras versiones: 39,95 €

Disponibilidad: Windows, macOS, Androide iOS

G Data impresiona con una muy buena detección de malware en el laboratorio y una buena detección en sitios web infectados. Por desgracia, el programa se limita demasiado a la protección antivirus. Por ejemplo, es el único software de la prueba, aparte de Microsoft Defender, que no incluye VPN. Y hay pocas funciones adicionales más.

- + Buena protección antivirus, muy buenas condiciones.
- − Equipamiento mínimo, algo complicado.

8 F-SECURE TOTAL

Precio: 99,99 €
Otras versiones: 49,99 €

Disponibilidad: Windows, macOS, Androide iOS

F-Secure también brilla con unos índices de detección muy buenos. Sin embargo, registró el mayor número de falsos positivos en la prueba y solo alcanzó una calificación pasable en protección contra phishing. Las escasas funciones, la fuerte ralentización del PC y el engorroso manejo impiden que el programa alcance una clasificación más alta.

- + Buena protección antivirus.
- − Mayor ralentización de la prueba, manejo complicado.

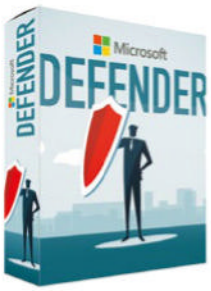
9 ESET HOME SECURITY ULTIMATE

Precio: 119,99 €
Otras versiones: 39,98 €

Disponibilidad: Windows, macOS, Android eiOS

ESET ocupaba el último puesto en 2024; este año no es el caso. ESET ha recuperado puntos de nota, aunque está ligeramente por detrás de Norton, a la par de muchos otros. Esto se debe principalmente a su detección de virus claramente mejorada. El hecho de que siga en noveno lugar se debe al precio. En cualquier caso, es un gran avance.

- + Buena protección antivirus, muy buena protección de datos.
- − Manejo complicado.



10 MICROSOFT DEFENDER

Precio: Gratuito
Otras versiones: No

Disponibilidad: Windows (incluido de serie)

Para ser un programa gratuito, Microsoft Defender lo hizo muy bien durante mucho tiempo. Ahora, la posición privilegiada le pasa factura. Aunque la protección básica de Windows tiene una buena detección de virus, sin conexión a Internet cae en picado. Tampoco ha superado la importante prueba de protección contra el phishing.

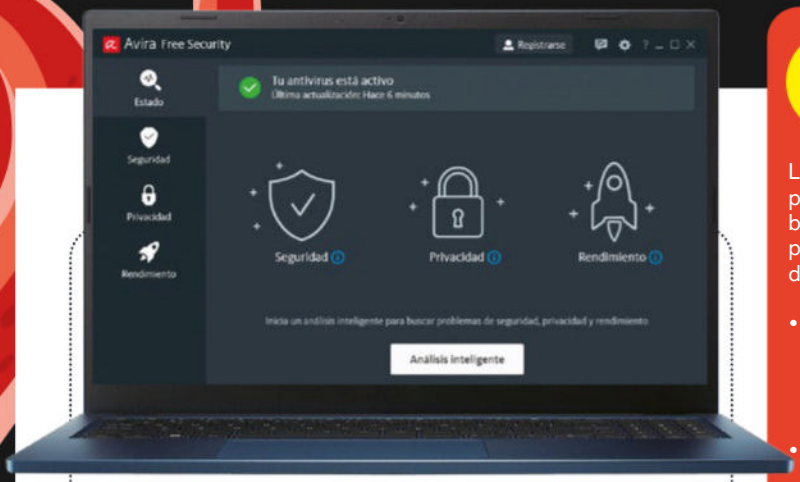
- + Buena protección antivirus.
- − Protección insuficiente sin Internet y contra el phishing.

Buena detección de malware en el laboratorio, incluso en sitios infectados, casi sin falsos positivos	8,60	Muy buena detección de malware en el laboratorio, incluso en sitios infectados, pocos falsos positivos	8,80	Muy buena detección de malware en el laboratorio, incluso en sitios infectados, muchos falsos positivos	9,00	Muy buena detección de malware en el laboratorio, incluso en sitios infectados, casi sin falsos positivos.	8,60	Buena detección de malware en el laboratorio, algo deficiente en sitios infectados, insuficiente sin Internet y contra el phishing, pocos falsos positivos	7,00
Cortafuegos, VPN, control parental, escáner de vulnerabilidades, asistente de actualizaciones, backup, eliminador de rastros, gestor de contraseñas	9,40	Cortafuegos, control parental, asistente de actualizaciones, backup, eliminador de rastros, gestor de contraseñas	6,00	Cortafuegos, VPN, gestor de contraseñas	5,40	Cortafuegos, VPN, control parental, protección antirrobo, asistente de actualizaciones, gestor de contraseñas	6,00	Cortafuegos, control parental, protección antirrobo, asistente de actualizaciones, eliminador de rastros, gestor de contraseñas	6,00
Inapreciable	9,60	Algo apreciable	8,40	Algo apreciable	8,20	Inapreciable	9,40	Algo apreciable	8,60
Manejo complicado, protección de datos inadecuada	4,00	Manejo algo complicado, muy buenas condiciones, buena protección de datos	7,20	Manejo complicado	5,20	Manejo complicado, muy buena protección de datos	6,40	Manejo complicado	5,20
Notable	8,20	**Notable**	8,20	**Notable**	8,20	**Notable**	8,20	**Bien**	7,00
42,99 €		**81,95 €**		**99,99 €**		**119,99 €**		**Gratuito**	

TRUCOS Y CONSEJOS

LAS PREGUNTAS MÁS IMPORTANTES

A la hora de comprar un antivirus hay que tener en cuenta algunas cosas. Aquí están las respuestas a las preguntas más importantes.



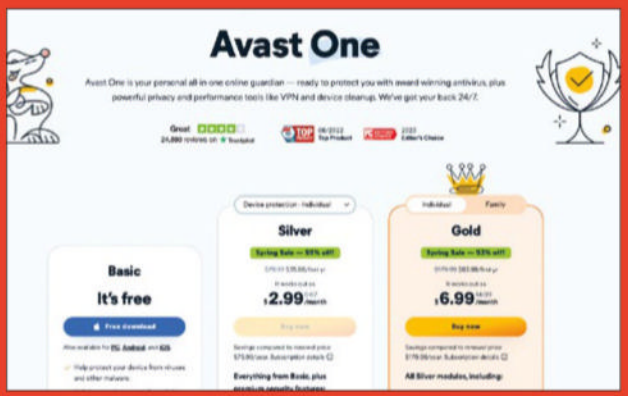
1 ¿QUÉ SISTEMAS LOS NECESITAN?

- **Windows:** este sistema es el principal objetivo de los ciberdelincuentes. Por tanto, la protección antivirus es imprescindible. Microsoft Defender y los programas gratuitos pueden considerarse una alternativa a los soluciones de pago.
- **macOS:** es más cerrado que Windows y es menos objetivo de los piratas informáticos debido a su uso menos extendido. Sin embargo, los usuarios de macOS son igual de susceptibles de sufrir phishing y fraude. Actualmente, cualquier dispositivo con macOS también debe protegerse de manera adecuada.
- **Android:** la situación de la seguridad en los dispositivos Android es particular. Esto se debe a que las aplicaciones pueden proceder de tiendas de terceros no controladas, y en estas hay pocas restricciones para las aplicaciones. Además, las actualizaciones para Android se lanzan en momentos diferentes o no llegan al terminal, dependiendo del fabricante del smartphone. Esto es algo ideal para los hackers. Por lo tanto, una aplicación antivirus es extremadamente recomendable.
- **iOS:** las aplicaciones en iOS son más limitadas y casi siempre proceden de la tienda oficial. Por lo que no es obligatorio un antivirus como tal. Sin embargo, los extras como una VPN, un gestor de contraseñas y otras funciones sí que resultan útiles.

2 PUNTOS A VALORAR ANTES DE COMPRAR

Lo más importante al comprar un programa antivirus es, por supuesto, que sea una protección fiable. Así que lo primero que debes hacer a la hora de decidir qué comprar es consultar la tabla de pruebas. Sin embargo, antes de sacar la cartera, hay que tener cuidado con algunas trampas que podrían costarte dinero:

- **Número de licencias:** los fabricantes ofrecen sus programas en distintos paquetes de licencias a precios diferentes. Según el número necesario, la diferencia puede superar los 100 €, como puede verse en la tabla de la página 52. Aparte está el smartphone, ya que las licencias también son válidas para Android e iOS.
- **Modelo de suscripción:** la mayoría de los fabricantes ofrecen licencias en forma de suscripción. Esto significa que se renuevan automáticamente al cabo de un año. En algunos casos, entonces hay que pagar un precio más alto. Por tanto, es importante saber de antemano si se va a contratar una suscripción, y si se puede desactivar o cancelar inmediatamente después de la compra. En ese caso, la licencia funcionará durante el tiempo ya abonado.
- **Paquete inteligente para ahorrar:** los paquetes de seguridad contienen distintas funciones según el fabricante. Si ya se usa un gestor de contraseñas, una VPN, un control parental o un programa de puesta a punto, puede tener bastante sentido comprar un paquete de protección que lo incluya todo, para así dejar que caduquen las demás licencias, ahorrando también dinero.



KIOSKEROS

3 ¿CUÁNDO USAR O NO UNO **GRATUITO**?

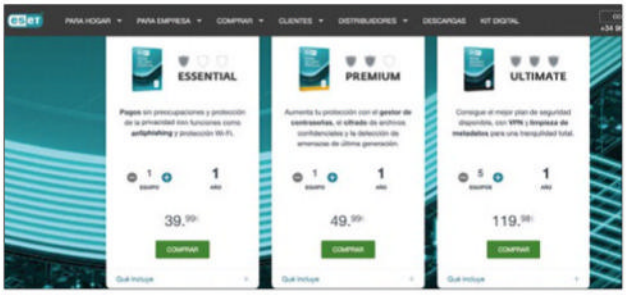
La conveniencia o no de gastar dinero en protección antivirus depende de lo que se le pida. Microsoft Defender ha recibido una nota de Bien en la prueba y cumple con las tareas más básicas y protege correctamente contra malware. Lo mismo ocurre con las versiones gratuitas de otros proveedores, que suelen ofrecer la misma detección de virus que las versiones de pago.

Los expertos opinan: los programas gratuitos no son una garantía en estos momentos. La principal amenaza para los particulares es ahora el phishing y el fraude. Por ejemplo, aparece una queja sobre un transportista de paquetes en Facebook y un usuario aporta su experiencia. Diez minutos después, un empleado de soporte del servicio de paquetería se pone en contacto, hace referencia al post y solicita los detalles del cliente en la página de la queja. También hay una recompensa de 10 € por hacerlo. Al abrir el enlace facilitado, la página parece auténtica. Datos como el IBAN para cobrar la recompensa son enviados, pero poco después el dinero desaparece de la cuenta del cliente. Un programa gratuito no suele darse cuenta de esto, pero los buenos avisan: reconocen que el enlace es sospechoso, que la página es falsa y pueden ver en el texto que se trata de un intento de fraude. También le informarán si los datos aparecen en la Darknet tras la denuncia. Además de esto, muchos fabricantes ofrecen asistencia en caso de reclamación.

4 ¿QUÉ **EXTRAS** OFRECE UNA SUITE COMPLETA?

Antes de comprarlo, hay que echar un vistazo a las características exactas del software. Estas aparecen en la página web del fabricante y, a menudo, difieren en las distintas variantes (véase la siguiente pregunta). Las características más importantes se pueden encontrar en la tabla del test. Funciones como gestor de contraseñas, copias de seguridad, asistente de actualizaciones, escáner de vulnerabilidades, VPN, protección para banca online y de identidad se recomiendan para cualquiera que no utilice otros programas. El control parental también es útil para los padres y otras funciones como la optimización del sistema operativo, la destrucción segura de datos, la protección al minar criptomonedas y las herramientas de cifrado solo son útiles para algunos usuarios. En la web del fabricante, se pueden comprobar las funciones más importantes para cada usuario y averiguar exactamente qué incluyen. Por ejemplo, hay grandes diferencias entre los distintos fabricantes cuando se trata de la identidad individual. Las mejores funciones adicionales en el campo de pruebas las ofrecen los programas Kaspersky Premium con la calificación de Sobresaliente; Bitdefender Ultimate Security un poco por debajo; y Norton 360 Advanced que prácticamente empata con el anterior en este apartado.

5 LAS DISTINTAS **ALTERNATIVAS**



Los programas antivirus están disponibles en diferentes paquetes que difieren en términos de funcionalidad. Cuál es el mejor para cada usuario depende de las preferencias particulares de este:

- **Antivirus:** según el fabricante, esta variante es gratuita y solo ofrece protección antivirus pura, sin extras. El ordenador está tan bien protegido contra malware como con las otras variantes. Estos paquetes son adecuados para profesionales que cubren las funciones que faltan con otro software.
- **Seguridad en Internet:** el paquete de gama media de la mayoría de los fabricantes ofrece todo lo que cabe esperar de un programa de protección. Normalmente, solo trae los extras importantes para la seguridad. Estos paquetes se dirigen a usuarios que buscan protección sin complicaciones.
- **Paquete completo:** las opciones más caras traen todo lo que ofrece el fabricante. Suelen incluir funciones adicionales como gestor de contraseñas, VPN u optimización. Sin embargo, también cuentan con extras de seguridad como protección de identidad. Se dirigen a todo el mundo y ofrecen una solución integral.

6 ¿UNA MALA NOTA DE LOS **TÉRMINOS LEGALES**?

Computer Hoy hace que un abogado compruebe tanto los términos y condiciones como la política de privacidad de todos los programas. Esta se refiere a los datos personales del usuario. Una mala puntuación significa que el proveedor recopila demasiados datos o los cede a terceros. Los términos y condiciones, por su parte, regulan el uso del programa y las responsabilidades. Una mala puntuación aquí significa que las cláusulas no son válidas o no responden a los intereses del cliente. Los fabricantes suelen traducir los documentos del inglés y adoptarlos sin adaptarlos a la legislación europea. Si una cláusula no es válida, puede sustituirse por lo que haya estipulado el legislador. Esto suele ser mejor para el usuario. Por tanto, ante un litigio con un fabricante cuyas condiciones generales son deficientes, merece la pena consultar a un abogado, en función de la cuantía del proceso.

> Cuando se adquiere un programa de protección, merece la pena analizarlo detenidamente y ahorrar.

Carlos Gombau
Redactor Jefe

KIOSKEROS

NordVPN · CyberGhost · ExpressVPN · HIDE me · MULLVAD VPN

KIOSKEROS

VPN PARA NAVEGAR TRANQUILO

¿EN INTERNET Y A SALVO?

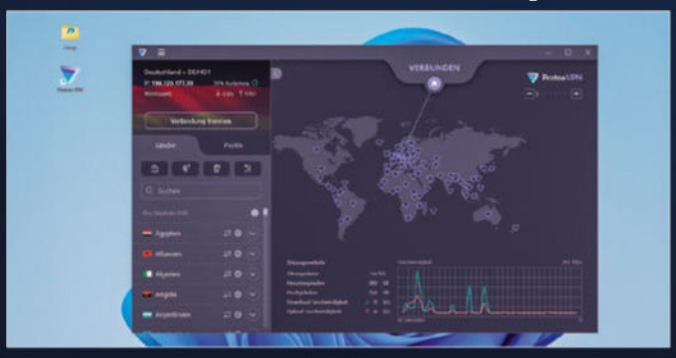
Protección de la privacidad en Internet y, además, streaming ilimitado: he aquí 10 servicios VPN para poder conseguirlo... cuando funcionan.

Al navegar con frecuencia con el PC, portátil, smartphone o tablet en redes WiFi inseguras, por ejemplo en cafeterías, hoteles o aeropuertos, los servicios VPN son una **herramienta útil para proteger la privacidad** frente al espionaje de terceros. Además, estas soluciones también pueden utilizarse para eludir los bloqueos geográficos. Así, con la dirección IP correcta, se puede ver Netflix en cualquier país o la televisión española en Helsinki. Todos los proveedores de VPN afirman tener la mejor protección contra el bloqueo. La cuestión es si esto es cierto. De ahí que toque analizar las promesas y lo que realmente funciona en el mundo de las VPN.

¿Qué es una VPN?

En pocas palabras, una red privada virtual es un servicio de privacidad. Su proveedor cifra todo el tráfico de datos de sus usuarios y, al mismo tiempo, oculta su identidad en Internet. La propia IP del usuario se sustituye por una nueva, opcionalmente por una extranjera.

Cuando el usuario navega por una página web, por ejemplo, esta solo ve la combinación numérica asignada por el proveedor de VPN. Sin embargo, el anonimato total no puede conseguirse ni siquiera con una VPN. Hoy en día, existen otras muchas formas de identificar y rastrear a los usuarios más allá de la dirección IP de Internet, como la huella digital del navegador. Sin embargo, una VPN hace que sea más difícil para los espías identificar a los usuarios y rastrear sus datos.



La interfaz de Proton VPN es de las más vistosas y elegantes del test.

Lo que las hace seguras

Los protocolos VPN utilizados son cruciales para la seguridad de un servicio de este tipo. La mayoría de los proveedores **trabajan con los métodos seguros** de tipo OpenVPN y WireGuard.

Un interruptor de emergencia (Kill-Switch), que desconecte la conexión a Internet en caso de problemas, también es esencial. Afortunadamente, ahora forma parte integrante de todos los programas VPN probados en este test. Pero no siempre está activado de fábrica. Con algunos proveedores, como Surfshark o Proton VPN, hay que activar Kill-Switch manualmente.

Apuntar también que en la prueba se observó que **todos protegen bien la IP** pública. Algunos servicios VPN incluyen funciones adicionales para ocultar aún mejor el rastro, como NordVPN o Proton VPN con sus servidores multisalto.

VPN: CIFRAS Y DATOS

26 %

de los españoles utiliza algún tipo de VPN

A nivel mundial, la cifra de usuarios sube hasta un 30 %.

76.000

millones de dólares

Es el valor de mercado previsto de los servicios VPN para finales de 2027. En 2022 solo rondaba los 45.000 millones de dólares estadounidenses.

39 %

de los usuarios de VPN son menores de 25 años

Por el contrario, solo el 16 % de los mayores de 55 años utilizan una VPN a nivel global.

43 %

utilizan las VPN por motivos de seguridad

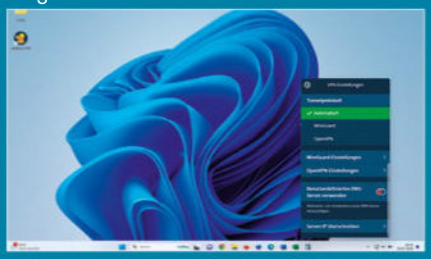
Mientras que el 26 % de todos los usuarios de VPN en el mundo las usan como servicios de ocultación para streaming.

OVPN · PrivadoVPN · ProtonVPN · Surfshark · windscribe

LO IMPORTANTE **ANTES DE CONTRATAR**

Antes de empezar, hay que pensar para qué se desea un servicio VPN. ¿Realmente mejorará la privacidad en Internet? ¿Es la herramienta perfecta para eludir los bloqueos de determinados países? Igual se buscan las dos cosas, pero es importante informarse antes:

- **Disponibilidad:** la mayor compatibilidad posible con dispositivos y el número permitido de conexiones simultáneas son importantes al utilizar la VPN en muchos equipos.
- **Seguridad:** el proveedor debe admitir protocolos OpenVPN o WireGuard, preferiblemente ambas tecnologías de cifrado.
- **Fiabilidad:** se debe elegir un proveedor de VPN que no almacene datos físicamente en unidades locales o en la nube, y que pueda demostrarlo con una auditoría.
- **Funciones:** muchas opciones no hacen que un servicio sea automáticamente mejor, pero lo preparan para diversos escenarios y perfiles de usuario diversos.
- **Geobloqueo:** para transmitir contenidos multimedia extranjeros, conviene un proveedor capaz de eludir los bloqueos de países.
- **Periodo de suscripción:** con la excepción de Mullvad VPN, todos los proveedores de VPN trabajan con modelos de suscripción. Los periodos más largos reducen significativamente los costes mensuales.



Los proveedores habituales admiten OpenVPN y WireGuard (aquí: Mullvad VPN).

Estas soluciones extra consiguen que los datos entrantes y salientes nunca pueden rastrearse hasta un único servidor. Sin embargo, el enganche pasa factura: la velocidad de conexión disminuye considerablemente.

Por otro lado, algunos proveedores también disimulan el hecho de que el usuario navegue con un servicio VPN. Esta tecnología, conocida como VPN furtiva, es especialmente útil en países restrictivos como China o Rusia, para así eludir la censura.

Quién se queda los datos

Apuntarse a un servicio VPN es un trueque. Ya no se regalan los datos privados de navegación al proveedor de Internet. Ahora se paga al de la VPN para que los gestione, ya que el tráfico pasa por sus servidores.

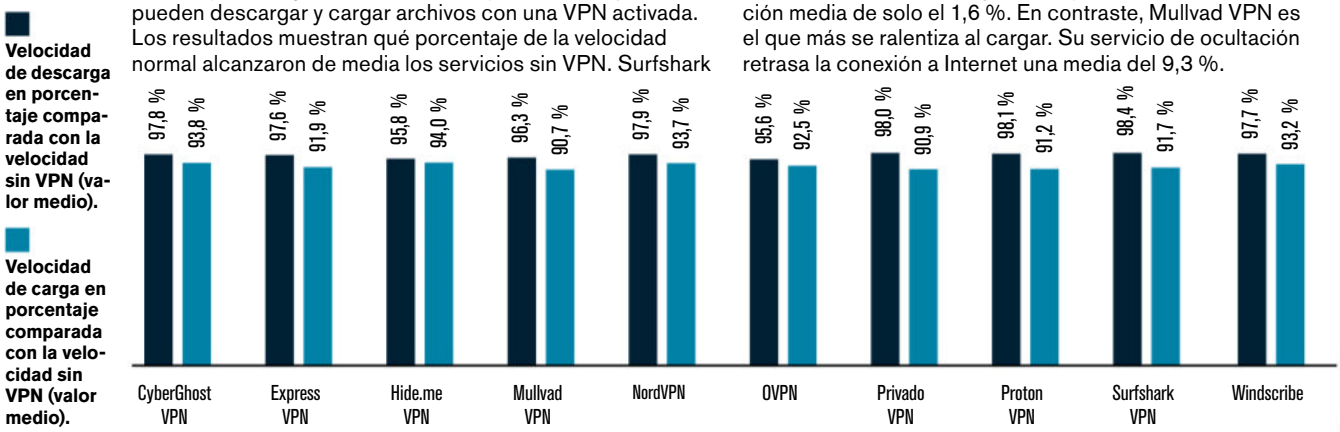
Por tanto, el proveedor de VPN debe tratar los datos del cliente de forma especialmente responsable. Casi todos los fabricantes afirman en sus **declaraciones sobre protección de datos** que no almacenan nada (política no-log). Sin embargo, esta audaz promesa publicitaria es engañosa. Por regla general, se trata de algo sensible, como las direcciones IP e información del tráfico entrante y saliente, que como mínimo permiten sacar conclusiones sobre el comportamiento del usuario. Sin embargo, los fabricantes también recogen otros datos, de forma limitada. Por ejemplo, algunos usan marcas de tiempo para registrar temporalmente cuántas conexiones VPN están activas. También recuerdan los datos de pago para que la suscripción permanezca abierta.

Es importante saber si los proveedores habían comprobado la seguridad de sus servicios y su política de no registro en **auditorías de seguridad externas**. Los cinco mejores servicios hacen un trabajo encomiable en este aspecto. Según expertos de seguridad independientes, las empresas no almacenan ningún dato sensible. Proveedores como OVPN, Windscribe o PrivadoVPN, por otro lado, apenas dejan que nadie mire sus informes. Algunos proveedores de VPN trasladan la sede de su empresa a un lugar situado fuera de la esfera de influencia de las alianzas de los servicios secretos (Five Eyes) o distribuidas en el extranjero para evitar la obligación de revelar datos. Por lo tanto, la ubicación del fabricante se incluye en la evaluación general.

Mullvad VPN ha elegido un enfoque interesante. El registro en el servicio se realiza mediante un número de cuenta generado aleatoriamente, por lo que no es necesario el clásico inicio de sesión con datos personales. Mullvad es también el único que permite pagar de forma completamente anónima

VELOCIDAD EN LAS PRUEBAS DE VPN

En Computer Hoy, se ha medido la rapidez con la que se pueden descargar y cargar archivos con una VPN activada. Los resultados muestran qué porcentaje de la velocidad normal alcanzaron de media los servicios sin VPN. Surfshark ofrece el valor de descarga más rápido, con una ralentización media de solo el 1,6 %. En contraste, Mullvad VPN es el que más se ralentiza al cargar. Su servicio de ocultación retrasa la conexión a Internet una media del 9,3 %.



EVITA EL **BLOQUEO DE PAÍSES** CON TU VPN

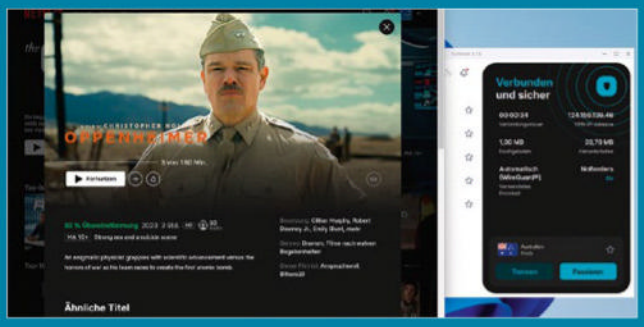
Hay muchas series y películas que tardan o no llegan a los servicios de streaming locales. Esto se debe a que los proveedores utilizan una herramienta llamada geobloqueo, para restringir los contenidos a determinadas regiones. Otros, en cambio, excluyen a los usuarios por completo cuando no viven en EE. UU. o Reino Unido, normalmente.

Las comprobaciones necesarias

Casi todos los proveedores de VPN anuncian que pueden superar los bloqueos por países de Netflix y compañía, para desbloquear toda la programación. Las pruebas han tenido diez regiones de Netflix como objetivo y varias bibliotecas multimedia extranjeras de Amazon Prime Video, Disney+, Paramount+, HBO Max, RaiPlay y BBC iPlayer. La redacción también ha comprobado si las retransmisiones en directo de canales como ARD y ZDF también funcionan a través de VPN. Como en otros países, Austria o Suiza, los grandes acontecimientos deportivos se retransmiten a menudo en directo por televisión en abierto, los servicios también tuvieron que demostrar su valía con las retransmisiones en vivo de ORF, ServusTV Austria y SRF.

NordVPN, Surfshark y ExpressVPN son los mejores para esto

Tres servicios han superado todas las pruebas de geobloqueo con un 100 % de éxito. NordVPN, Surfshark y ExpressVPN son, por tanto, especialmente adecuados para usuarios con servicios de streaming. En principio, todos los proveedores de VPN tienen ahora el problema en su radar y hacen el trabajo satisfactoriamente. Sin embargo, al centrarse específicamente en Netflix, Hide.me, Mullvad VPN y PrivadoVPN, todavía tienen algunos deberes que hacer para que sean recomendables.

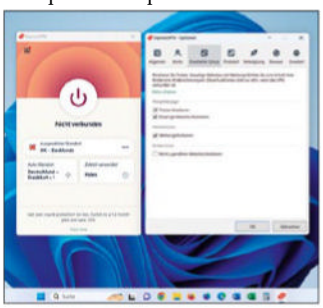


en efectivo. Basta con seleccionar el plazo deseado y enviar la cantidad requerida por carta a la dirección de la empresa, que está localizada en Suecia.

Los servidores que solo utilizan memoria que **se borra con cada reinicio** son una tendencia actual. Así, aunque se hayan registrado datos sensibles, desaparecen como muy tarde cuando se interrumpa el suministro eléctrico. ExpressVPN (Trusted Server) es el pionero de este desarrollo, y la mayoría de los proveedores analizados se han subido al carro y dirigen el tráfico de datos a través de servidores sin discos duros.

La velocidad baja con su uso

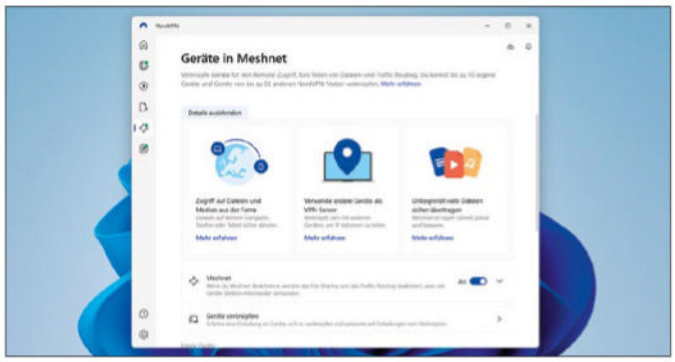
Los servicios VPN rara vez utilizan todo el ancho de banda del que se dispone. Una de las razones es la mayor **distancia hasta los servidores** VPN. Sobre todo si están situados lejos, en el extranjero. El cifrado también pasa factura.



Activa el Gestor de amenazas de ExpressVPN, para protegerte de los peligros que te acechan en línea.

Se han sometido todos los servicios a una prueba de resistencia de 24 h en un servidor local y se han medido los valores de descarga, carga y tiempos de respuesta del servidor (ping). La mayoría de los servicios solo ralentizaron ligeramente las descargas. Surfshark fue especialmente rápido. Incluso el proveedor más lento, OVPN, ofreció una buena relación calidad/precio con una pérdida de velocidad aceptable de alrededor del 4,4 %.

Todos los servicios fueron más flojos en el envío. Aquí se observan caídas de hasta el 9 %, siendo Mullvad VPN y PrivadoVPN los que más sufrieron. Las mayores diferencias se dieron en el ping. CyberGhost se distanció de todos los demás con unos fenomenales 9 ms. Al medir el mayor retardo, este se dio en NordVPN con una media de 25 ms, lo cual no deja de ser satisfactorio: es suficiente para streaming y videoconferencias, aunque no resulta recomendable para juegos rápidos online.



Con la función Meshnet (también disponible gratuitamente), se puede crear un túnel de datos cifrados entre dos o más dispositivos con NordVPN. Es parte de un paquete repleto de extras para todo tipo de usuarios.

¿Qué es lo más importante?

Una buena cobertura hace que el servicio pueda utilizarse con garantías. Los fabricantes también equipan sus servicios de ocultación con todo tipo de extras. Por ejemplo, NordVPN es popular por su función Meshnet para crear una LAN privada virtual. Y el Gestor de amenazas de ExpressVPN bloquea rastreadores no deseados y sitios web maliciosos. Por su parte, Surfshark proporciona automáticamente una nueva dirección de camuflaje cada 5 min con su Rotating IP.

CONCLUSIÓN

Ninguno de los proveedores probados presentaba fallos de seguridad reales. NordVPN gana la prueba una vez más con su sólido rendimiento. Surfshark es una potente alternativa hacia una mejor privacidad, más económica y con una configuración muy sencilla.

> NordVPN gana esta prueba. Ningún otro servicio ofrece un paquete que lo supere globalmente.

Carlos Gombau
Redactor Jefe

LA PRUEBA EN DETALLE

Los servicios VPN difieren no solo en términos de seguridad, características y velocidad, sino también en cuanto a la eficacia con que el sistema de ocultación anula los bloqueos por países.

1 NORD SECURITY
NORDVPN
Precio: 71,26 €

Sede: Panamá
Compatibilidad: Windows, macOS, Linux, Android, iOS y otros

Con un paquete global de seguridad robusta, una promesa creíble de protección de datos y una enorme infraestructura, NordVPN se aseguró la victoria en la prueba. El servicio furtivo no solo funciona con la última tecnología y brilla cuando se trata de streaming, sino que también marca sus propio estilo con extras como Meshnet.

+ VPN premium con numerosos extras.

− No hay versión gratuita, ligeras deficiencias en el ping.

2 SURFSHARK
SURFSHARK VPN
Precio: 49,80 €

Sede: Países Bajos
Compatibilidad: Windows, macOS, Linux, Android, iOS y otros

Con una facilidad de uso inigualable, una infraestructura rápida y amplia, y potentes funciones de ocultación, Surfshark demuestra que los buenos servicios VPN no tienen por qué ser caros. El rendimiento de streaming también es excelente y el servicio hace un trabajo bueno con los geobloqueos de Netflix y otros.

+ Precio ajustado y sin límites de conexión.

− Kill-Switch se debe activar manualmente.

3 CYBERGHOST
CYBERGHOST VPN
Precio: 67,76 €

Sede: Rumanía
Compatibilidad: Windows, macOS, Linux, Android, iOS y otros

CyberGhost impresiona sobre todo por su velocidad en los test. También gana puntos con su facilidad de manejo y numerosos servidores especiales enfocados al uso en streaming y juegos online. Sin embargo, la falta de funciones como Multi-Hop y app split tunnelling bajo Windows le cuestan al proveedor valiosos puntos.

+ Buena velocidad, servidor especial para streaming.

− Sin multisalto, también faltan funciones para VPN invisible.

4 PROTON
PROTON VPN
Precio: 71,88 €

Sede: Suiza
Compatibilidad: Windows, macOS, Linux, Android, iOS y otros

La política de protección de datos es ejemplarmente transparente, e incluso las aplicaciones son de código abierto. WireGuard también está incluido. En términos de seguridad, el fabricante ha añadido funciones de ofuscación que engañan a las autoridades. Por desgracia, esto hace los menús bastante confusos y desordenados.

+ Servidor Tor propio, alta transparencia.

− Menús algo confusos, sin servidor solo en RAM.

5 EXPRESSVPN
EXPRESSVPN
Precio: 91,82 €

Sede: Islas Vírgenes Británicas
Compatibilidad: Windows, macOS, Linux, Android, iOS y otros

Es el servicio más caro de la prueba. Sus puntos fuertes son la potencia y facilidad de uso. ExpressVPN también utiliza servidores respetuosos con la privacidad y se puede usar en muchos dispositivos cliente. En negativo, las características del proveedor son más bien espartanas y la falta de WireGuard también se considera un defecto.

+ Amplia compatibilidad de dispositivos, muy bueno para streaming.

− Pocas funciones adicionales, precio elevado.

	NordVPN	Surfshark	CyberGhost	ProtonVPN	ExpressVPN
SEGURIDAD Y FIABILIDAD					
	Protocolos seguros, política de no registros verificada, servidores solo RAM — 9,80	Protocolos seguros, política de no registros verificada, servidores solo RAM — 9,20	Protocolos seguros, política de no registros verificada, pero sin Multi-Hop — 8,00	Protocolos seguros, política de no registros verificada, pero sin servidores solo RAM — 7,80	Política de no registros verificada, servidores solo RAM, pero sin soporte de WireGuard — 8,20
VELOCIDAD					
	Descargas rápidas, debilidades en la subida y el ping — 8,40	Descargas muy rápidas, buen ping, debilidades en la subida — 8,40	Descargas rápidas, muy buen ping, debilidades en la subida — 8,80	Descargas rápidas, buen ping, debilidades en la subida — 8,20	Descargas rápidas, muy buen ping, debilidades en la subida — 8,40
STREAMING DE CONTENIDOS CON GEOBLOQUEO					
	Desbloquea muchas bibliotecas de medios extranjeras y transmisiones en vivo — 10,00	Desbloquea muchas bibliotecas de medios extranjeras y transmisiones en vivo — 10,00	Desbloquea muchas bibliotecas de medios y transmisiones en vivo, pero no Disney+ — 8,40	Desbloquea muchas bibliotecas de medios extranjeras y transmisiones en vivo — 9,80	Desbloquea muchas bibliotecas de medios extranjeras y transmisiones en vivo — 10,00
DISPONIBILIDAD Y EQUIPAMIENTO					
	111 países, 10 conexiones paralelas, muchos extras — 9,00	100 países, sin límite de conexiones, muchos extras — 8,60	100 países, 7 conexiones paralelas, pocos extras — 6,80	100 países, 10 conexiones paralelas, pocos extras — 7,20	105 países, 8 conexiones paralelas, pocos extras — 5,60
FACILIDAD DE USO Y COMODIDAD					
	Fácil, lista de países algo escondida — 8,40	Muy fácil, estructura clara — 9,60	Fácil, algunas funcionalidades algo escondidas — 8,40	Algo complicado, muchas funciones solo para avanzados — 6,80	Muy fácil, estructura clara — 9,2
	Notable 9,20	Notable 9,00	Notable 8,20	Notable 8,20	Notable 8,20
	71,26 €	49,80 €	67,76 €	71,88 €	91,82 €

COMPUTER HOY RESPONDE:

Protocolo VPN
El protocolo VPN define reglas y procesos con los cuales los servicios de este tipo establecen una conexión segura. Convierten paquetes de datos en un protocolo VPN y luego los transmiten a Internet.

Kill-Switch
Es una especie de interruptor de emergencia que desconecta automáticamente la conexión a Internet si una conexión VPN falla o se interrumpe. El Kill-Switch no siempre está activado por defecto.

Multi-Hop
Esta técnica que se conoce como multisalto envía datos que no van a través de un solo servidor VPN, sino que lo hacen por al menos dos consecutivos. Así, la información del usuario es más difícil de rastrear.

STEALTH-VPN (ofuscación)
Modo de ocultación que camufla el flujo de los datos. La información aparece como tráfico de Internet que no se distingue del normal. Esto permite eludir censores que pueden reconocer al proveedor de VPN.

6 EVENTURE
HIDE.ME VPN
Precio: 65,44 €

Sede: Malasia
Compatibilidad: Windows, macOS, Linux, Android, iOS y otros

Ofrece mucha libertad a la hora de organizar la privacidad online. A pesar de las mejoras en la interfaz de usuario, el funcionamiento sigue estando reservado a usuarios avanzados y no ofrece auditoría. Sin embargo, la velocidad es bastante rápida y gana en la elección de protocolos, con el servicio de ocultación de Malasia.

- \+ Muchos protocolos, también apto para descargas torrent.
- − Funcionamiento algo complicado, puntos débiles con Netflix.

7 OVPN
OVPN
Precio: 59,88 €

Sede: Suecia
Compatibilidad: Windows, macOS, Linux, Android, iOS y otros

Hace algunas cosas muy bien, pero no convence en todos los aspectos. El servicio VPN sueco se basa en tecnologías modernas como WireGuard y servidores solo en RAM. Sin embargo, la selección de países es muy reducida y hay margen de mejora en cuanto a funciones y disponibilidad de dispositivos. El funcionamiento es agradablemente sencillo.

- \+ Soporte WireGuard, buena velocidad.
- − Pocas funciones, sin auditoría de seguridad.

8 MULLVAD
MULLVAD VPN
Precio: 60,00 €

Sede: Suecia
Compatibilidad: Windows, macOS, Linux, Android, iOS y otros

Cuando se trata de los importantes criterios VPN de discreción y protección de la privacidad, Mullvad VPN muestra su lado fuerte y puntúa alto con su tecnología bien blindada. Las opciones de pago anónimo son otra de sus bazas. Sin embargo, la VPN furtiva ofrece menos ubicaciones y características más pobres que las mejores alternativas.

- \+ Muy buena seguridad y transparencia, pago en efectivo.
- − Selección de funciones algo reducida, con solo algunos extras.

9 WINDSCRIBE
WINDSCRIBE
Precio: 63,39 €

Sede: Canadá
Compatibilidad: Windows, macOS, Android, iOS y otros

En general, Windscribe es uno de los mejores proveedores de VPN, pero el servicio no se puede recomendar sin reservas. El menú principal es demasiado reducido y las funciones resultan a veces incomprensibles. Por otro lado, Canadá como ubicación para la sede de la empresa no es la primera opción cuando se trata de maximizar la privacidad.

- \+ VPN rápida, sin límites de conexión.
- − Funcionamiento complicado, localización en un país Five Eyes.

10 PRIVADO NETWORKS
PRIVADOVPN
Precio: 44,85 €

Sede: Suiza
Compatibilidad: Windows, macOS, Android, iOS y otros

La base técnica es buena con OpenVPN y WireGuard, y la velocidad de las conexiones VPN también es rápida. Sin embargo, los extras son un poco escasos y el hecho de que PrivadoVPN anuncie una protección de datos estricta, pero no tenga esta promesa confirmada por empresas de pruebas externas, ya no está al día en 2024.

- \+ Versión gratuita disponible, precio favorable.
- − Pocas funciones adicionales, sin auditoría.

Protocolos seguros, pero sin servidores solo RAM y sin auditoría	7,00	Protocolos seguros, servidores solo RAM, pero sin auditoría	8,40	Protocolos seguros, política de no registros verificada, servidores solo RAM, pago anónimo	10,00	Protocolos seguros, servidores solo RAM, ubicación en Five Eyes y sin auditoría	5,60	Protocolos seguros, pero sin servidores solo RAM, sin Multi-Hop y sin auditoría	5,40
Descargas rápidas, muy buen ping, debilidades en la subida	8,20	Descargas rápidas, buen ping, debilidades en la subida	7,80	Descargas rápidas, buen ping, ligeras debilidades en la subida	7,80	Descargas rápidas, muy buen ping, debilidades en la subida	8,60	Descargas rápidas, buen ping, ligeras debilidades en la subida	8,20
Desbloquea muchas bibliotecas de medios y transmisiones en vivo, flojea en Netflix	9,20	Desbloquea muchas bibliotecas de medios y transmisiones en vivo, flojea en Netflix	8,60	Desbloquea solo algunas bibliotecas de medios y transmisiones en vivo	6,00	Muy bueno para Netflix, pero flojea en Disney+ y Paramount+	8,80	Desbloquea solo algunas bibliotecas de medios y transmisiones en vivo	6,60
56 países, 10 conexiones paralelas, muchos extras	8,20	21 países, 5 conexiones paralelas, pocos extras	4,60	41 países, 5 conexiones paralelas, pocos extras	4,40	69 países, sin límite de conexiones, pocos extras	7,00	49 países, 10 conexiones paralelas, pocos extras	5,60
Algo complicado, algunas funciones solo para avanzados	7,20	Muy fácil, estructura clara	9,20	Fácil, pero muy pocas funciones de comodidad	5,20	Algo complicado, mala traducción de los textos del menú	6,00	Fácil, pero diseño del menú poco amigable para la vista	8,40
Notable	**8,00**	**Notable**	**7,80**	**Notable**	**7,40**	**Notable**	**7,40**	**Bien**	**6,60**
65,44 €		**59,88 €**		**60,00 €**		**63,39 €**		**44,85 €**	

LA CRIPTOGRAFÍA EVOLUCIONA

¿ES SEGURO ALMACENAR NUESTRA VIDA EN LA NUBE?

La criptografía sigue evolucionando y se adapta a la era digital actual para garantizar la privacidad de los datos, una computación verificable y lograr la seguridad en la nube.

Quien tiene la información tiene el poder". La frase es del filósofo Thomas Hobbes. Pero Hobbes no se refería a la información en términos generales sino al **acceso a la información privilegiada**, oculta, en exclusiva. Se podría decir que entrar en la nube, hackear el almacén digital de nuestra vida, es como entrar en Troya.

Las máquinas no son nuestras

La ubicuidad de Internet y la computación en la nube hacen cada vez más común almacenar y procesar datos en máquinas de terceros. Eso es la nube: un espacio en las súper máquinas de otros. Tenemos que confiar en que las máquinas de terceros son honestas en todo momento, ¡incluso si son pirateadas! Pero esto no es realista y se contradice con los numerosos incidentes de seguridad que se denuncian periódicamente.

El gran desafío es inventar una nueva generación de protocolos criptográficos para computación segura en máquinas que no son de confianza, de una manera que sea rentable. Y así, **la computación verificable es una nueva rama de la criptografía** que ha llegado para quedarse. Es la base para que la nube, que usamos para almacenarlo todo –fotos, archivos, documentos–, sea realmente confiable y lo siga siendo al mismo tiempo que también avanzan las técnicas de los hackers.

La computación verificable no solo se encargará de solucionar problemas existentes sino que favorecerá la creación de nuevas tecnologías que a día de hoy son inimaginables.

El papel histórico de la criptografía

La criptografía ha existido durante milenios como mecanismo para ocultar mensajes. Julio César utilizó técnicas criptográficas en el siglo I a. e. c. para enviar mensajes tácticos cifrados que le permitieron ganar guerras e hicieron imparable al que, tras su muerte, fue el gran Imperio romano.

La criptografía también desempeñó un papel crucial para lograr el fin de la Segunda Guerra Mundial. Alan Turing y su equipo en Bletchley Park consi-

Foto: Depositphotos.com

Enigma: se trataba de una máquina electromecánica de cifrado rotativo.

KIOSKEROS

guieron **romper el cifrado de los mensajes** de la Alemania nazi y su máquina ENIGMA, basándose en estudios previos de matemáticos polacos.

En el siglo XXI las aplicaciones de la criptografía nos permiten comunicarnos con nuestros familiares y amigos en aplicaciones de mensajería instantánea, como WhatsApp, sin que nadie nos espíe, o comprar por Internet de manera segura sin riesgo de que un tercero pueda acceder a nuestros datos bancarios.

Un nuevo papel para la criptografía

La criptografía moderna no se limita a proteger secretos durante la comunicación. Existe un campo de investigación emergente que se ocupa de resolver la pregunta: ¿cómo puedo delegar un trabajo a alguien y estar seguro de que se realiza correctamente sin tener que rehacerlo yo mismo? Aplicándolo a la nube: ¿cómo podemos dejar nuestros datos en la máquina de otros y estar seguros? Para resolver este problema, los criptógrafos trabajan en el cálculo verificable, una nueva clase de criptosistemas. Este enfoque se basa en el concepto de prueba, pilar de las matemáticas desde hace milenios. Una prueba es una secuencia de pasos lógicos que permite asegurar la veracidad de una afirmación. Por ejemplo, se puede demostrar el saldo de una cuenta bancaria dando los valores intermedios del saldo después de cada transacción. Sin embargo, una prueba de este tipo es tan larga como el tiempo de cálculo del resultado, es decir, demasiado lenta de comprobar y, por tanto, inútil si el objetivo original era pedir a otra persona que hiciera el trabajo.

Para superar este obstáculo, la computación verificable **se basa en pruebas probabilísticas**. Simplificando mucho, se trata de sistemas con dos actores –el que prueba y el verificador– que proporcionan un método que convence al verificador de su validez inspeccionando únicamente una pequeña parte del proceso.

Imposible hacer trampas

De este modo, la verificación del cálculo es rápida. Pero ¿es seguro un método así? Aquí es donde entra en juego la criptografía para desempeñar un papel crucial, dado que garantiza que es prácticamente imposible hacer trampas sin ser descubierto, incluso si el cálculo y la prueba probabilística son generados por un atacante.

La computación verificable ha progresado significativamente en los últimos 10 años, pasando de la teoría pura a las **primeras aplicaciones prácticas**.

El proceso de lograr abaratar el sistema

El principal obstáculo para la adopción generalizada de esta tecnología es el coste de generación de las pruebas, que se encarece rápidamente cuando se usa sobre grandes cantidades de datos. Sin embargo, los criptógrafos de todo el mundo trabajan por mejorar esta tecnología. Este es, por ejemplo, uno de los objetivos del proyecto PICOCRYPT que ha recibido financiación del European Research Council (ERC).

Recientemente, ha sido presentado un resultado científico que muestra una solución novedosa para la ejecución verificable de redes neuronales. Aplicaciones como ChatGPT, el reconocimiento facial o las recomendaciones de contenido personalizadas que realizan empresas como Instagram, TikTok o Netflix son solo algunos ejemplos de las múltiples aplicaciones de estas redes.

A través de la computación verificable cualquier dispositivo podría utilizar la nube sin tener que confiar en ella, simplemente podría pedir una prueba del trabajo que delega. Esto es por ejemplo lo que ocurre cuando utilizamos un servicio de correo electrónico o usamos ChatGPT. La magia de estos protocolos no acaba aquí. Algunos de ellos gozan de una propiedad adicional llamada conocimiento cero, que implica que las pruebas no revelan ninguna información sobre su contenido.

Lo servicios cloud son muy útiles. Por ejemplo, para liberar memoria en nuestros dispositivos o para acceder a la información desde cualquier lugar.

Conocimiento cero

Las pruebas de conocimiento cero permiten aplicaciones aún más disruptivas, porque pueden **garantizar la privacidad a la entidad** que genera la prueba. Por ejemplo, la nube podría demostrar la exactitud de una tarea de inteligencia artificial sin temor a filtrar los secretos de su algoritmo, que es información privada muy valiosa. O, con otro ejemplo, si fuéramos a alquilar una casa, el arrendador querrá saber que tenemos solvencia financiera suficiente para poder cumplir con los pagos. Es costumbre pedir la última renta o incluso avales bancarios pero ¿no estamos dando demasiada información? Gracias a las **pruebas de conocimiento cero**, es posible demostrar a un arrendador que nuestros ingresos mensuales superan la cuantía del alquiler sin revelar el cómputo total de nuestra nómina, que es todo lo que necesita saber.

En cualquier caso, la criptografía evoluciona en la era digital. Troya ya no es un caballo de madera, y los muros para protegernos han de estar a la altura.

Dario Fiore
IMDEA SOFTWARE
theconversation.com

Foto: Depositphotos.com

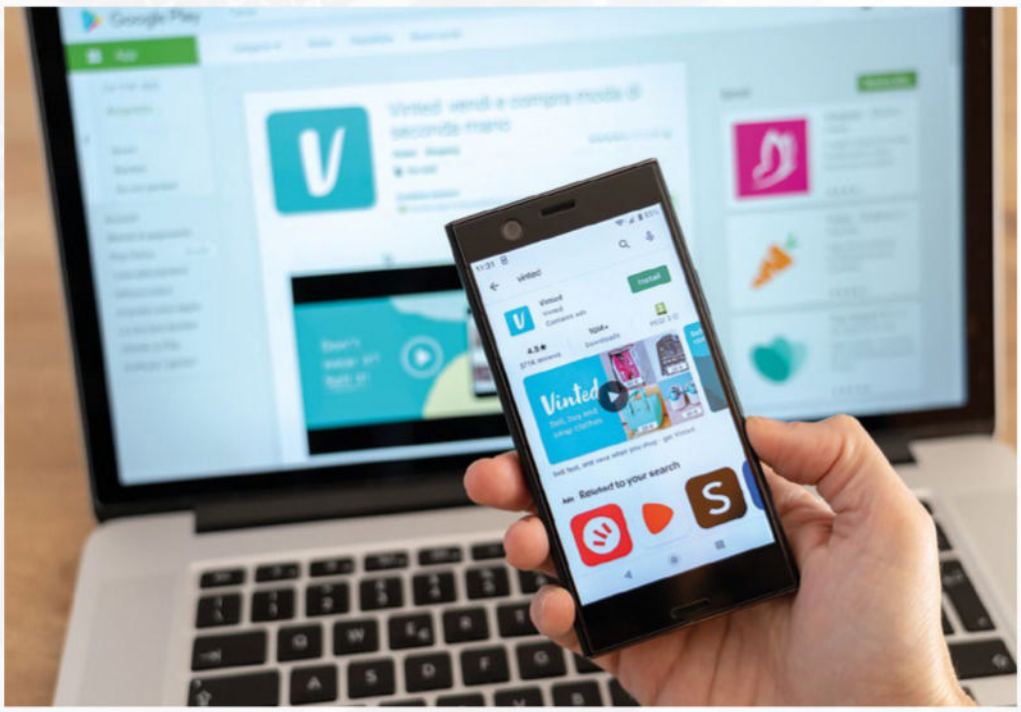
Los piratas pueden obtener datos cifrados e, incluso, conocer el método de codificación, pero sin la clave les será imposible descifrar el código.

LAS APLICACIONES MÓVILES DATOS PRIVADOS SIN QUE

En la economía digital, la privacidad es crucial. Los datos personales otorgan poder a unas pocas empresas que lideran este sector tan importante. Ante este panorama, los usuarios debemos ser siempre críticos y responsables en todas nuestras decisiones digitales.

En la Cuarta Revolución Industrial, basada en la economía digital, la generación de valor se centra en la personalización y los sistemas de recomendación, alimentados por la recopilación y también por el **procesamiento masivo de datos personales**.

Como expresó Clive Humby en el año 2006, los datos son el nuevo petróleo. En este sentido, asistimos resignados al crecimiento exponencial de los beneficios de muy pocas empresas tecnológicas, que ofrecen servicios 'gratuitos". Bien sabemos que no es así y que, aunque es mucho lo que ofrecen los nuevos servicios digitales en cuanto a contenidos, posibilidad de comunicación y alcance extraordinario, también es grande el riesgo continuo al que nos exponemos.


Vinted
Vinted
Vinted

COMPARTEN NUESTROS LO SEPAMOS

Hay que ser cuidadosos con la información que facilitamos, ya que cada dato que compartimos puede ser usado de una manera que no podemos controlar.

Grandes empresas podrían estar recopilando nuestros datos personales para fines comerciales y para incrementar su poder en la economía digital.

tecnológicas y posteriormente añadidas por los desarrolladores. Estas a veces realizan comportamientos adicionales en segundo plano (como la recolección y envío de datos personales), que pasan inadvertidos para el usuario e, incluso, a menudo, para el propio desarrollador.

Su desconocimiento supone, en cualquier caso, un **riesgo para la privacidad de los usuarios** y un riesgo económico para los responsables de la aplicación, ya que sin saberlo podrían estar incumpliendo la ley de protección de datos y ser sancionados con multas millonarias.

Los ciberguardianes de tus datos personales

El proyecto autoGDPR, liderado por investigadores de la UPM, trata de abordar estos problemas. Por un lado, implementa tecnologías de ciberseguridad que permiten observar el comportamiento de las aplicaciones móviles. Con ello pueden saber qué datos personales se recogen, a dónde se envían y si además estarían potencialmente incumpliendo la ley.

Esta tecnología puede ser utilizada por las agencias de protección de datos para tener evidencias de estos incumplimientos. También, por los desarrolladores, ya que podrán informarse a través de la página web del proyecto (aún en desarrollo) sobre qué hace su aplicación, para de este modo poder corregirlo y adherirse a la ley. Por su parte, los usuarios podrán conocer los detalles de cómo se comporta cada aplicación respecto a su privacidad y tomar una decisión informada antes de descargarla o utilizarla.

Este proyecto y las tecnologías que integra ya han dado lugar a estudios muy relevantes, que demuestran cómo más del 80 % de las aplicaciones que envían datos personales podrían estar **incumpliendo la ley de protección de datos**, al enviarlos a empresas como Google o Meta sin el conocimiento de los usuarios.

Tus datos importantes, en manos de 10 empresas

Además, se envían en la mayoría de las ocasiones a países fuera de la Unión Europea, con medidas de privacidad y protección de datos más laxas. Ciertos estudios reflejan que casi tres cuartas partes de los datos personales terminan en manos de sólo diez organizaciones, confiriéndoles un gran poder.

El primer requisito para lograr un entorno digital más seguro requiere que los desarrolladores y responsables de las aplicaciones sean transparentes con sus prácticas de privacidad, lo que será impulsado con el proyecto autoGDPR. Pero la responsabilidad de proteger nuestra privacidad digital recae también en nosotros mismos, los usuarios. Debemos ser diligentes, críticos y selectivos sobre las aplicaciones que descargamos y los servicios digitales que utilizamos. Es fundamental desempeñar un rol activo, leyendo y comprendiendo las políticas de privacidad, ajustando nuestras configuraciones para maximizar la protección y apoyando a aquellas empresas y aplicaciones que demuestran un compromiso genuino con la protección de los datos de sus usuarios.

Recordemos que cada acción en el mundo digital deja una huella. Es nuestro derecho y deber decidir cuán grande y visible queremos que sea. **Hagamos de nuestra privacidad una prioridad** porque, en el gran esquema de la economía de datos, el poder más significativo reside en las elecciones cotidianas de individuos informados.

Celia Fernández Aller y David Rodríguez Torrado
Universidad Politécnica de Madrid (UPM)
theconversation.com

LAS PRIMERAS 24 HORAS EN UN HIPOTÉTICO CORTE GLOBAL DE INTERNET

La interrupción global de Internet afectaría gravemente la comunicación, la economía y la seguridad. Dependemos de cables submarinos para transmitir datos, pero son vulnerables.

En los últimos años, ha aumentado la preocupación por la actividad militar rusa en torno a los cables submarinos que forman la columna vertebral de Internet, un entramado de 500 cables submarinos que se extienden a lo largo de cientos de miles de kilómetros, transmitiendo terabits de datos por segundo. Transportan el 97 % de las comunicaciones globales y son esenciales para transmitir datos **gubernamentales, financieros y personales**. La amenaza de un ataque coordinado podría generar interrupciones masivas en las comunicaciones globales, afectando tanto a civiles como a operaciones militares.

Aunque resultan esenciales, estos cables son sorprendentemente vulnerables. **Cada año se reportan alrededor de 100 cortes**, generalmente causados por accidentes con anclas o actividad pesquera. ¿Qué ocurriría si todo el Internet global dependiente de estos cables se cortara repentinamente?

Foto: Depositphotos.com

Internet se ha convertido en una herramienta indispensable para llevar a cabo las actividades diarias, tanto en el ámbito laboral como en el personal.

Minuto 1: El desconcierto inicial

Durante el primer minuto, la mayoría de las personas no nota la falta de Internet. Las aplicaciones y servicios que no requieren conexión siguen funcionando. Solo quienes intentan enviar un mensaje o actualizar una página web se dan cuenta de que algo anda mal. Las operaciones básicas en empresas y hogares continúan, aunque algunos **sistemas dependientes de la nube** empiezan a mostrar fallos. Los servicios críticos que dependen de datos en tiempo real, como los centros de control de tráfico y hospitales, podrían ver un ligero retraso en sus sistemas internos.

KIOSKEROS

5 minutos: La sospecha

A los cinco minutos, el problema se hace más evidente. Las redes sociales no actualizan, los mensajes no se envían y quienes dependen de Internet para trabajar comienzan a preocuparse. Los servicios de mensajería y las plataformas de videollamadas fallan, afectando la comunicación personal y profesional. **Los sistemas críticos,** como los hospitales y las fuerzas de seguridad, comienzan a activar sus planes de contingencia y a usar comunicaciones por radio y satélite para lograr coordinarse.

30 minutos: Crece la preocupación

Media hora después, el impacto es más palpable. Las líneas telefónicas se saturan mientras las personas intentan comunicarse con amigos y familiares. Las **tarjetas de crédito y débito** dejan de funcionar en tiendas y gasolineras, provocando largas filas y confusión. Los bancos se llenan de gente intentando retirar efectivo, anticipando problemas mayores. Los sistemas de control de tráfico y la logística de transporte pueden verse afectados, ralentizando la movilidad y la distribución de productos esenciales.

1 hora: Caos en los servicios críticos

Después de una hora sin Internet, el impacto en los servicios críticos se vuelve más evidente. Los sistemas hospitalarios sin acceso a historiales clínicos digitales deben recurrir a registros en papel, lo que ralentiza la atención y aumenta el riesgo de errores médicos. Las comunicaciones entre fuerzas de seguridad se limitan a sistemas de **radio y teléfonos satelitales**, que no pueden cubrir todas las necesidades de coordinación. En los bancos, la falta de acceso a redes digitales bloquea las transacciones y provoca un caos en las sucursales.

Foto: Wikimedia Commons **Autor:** Emil Neuerer, DJ4PI

Típica estación de comunicaciones de un radioaficionado. Este sistema puede resultar esencial en un corte mundial de Internet, manteniendo las conexiones.

6 horas: Crisis económica y social

La falta de Internet durante seis horas paraliza la economía. Los mercados financieros no pueden operar, causando pánico entre los inversores. El comercio electrónico y las plataformas de pago en línea se detienen por completo. Las estaciones de servicio no pueden aceptar pagos electrónicos y dejan a muchos conductores sin combustible. Los sistemas de seguridad que dependen de Internet, como cámaras de vigilancia y alarmas, dejan de funcionar y aumenta el riesgo de robos y vandalismo.

12 horas: Desesperación y vulnerabilidad

A las doce horas, la situación es crítica. Las únicas fuentes de información son la radio y, en algunos casos, la televisión, pero incluso estos medios comienzan a fallar debido a la **falta de infraestructura digital**. Los servicios de emergencia se ven saturados y desbordados ante la imposibilidad de comunicarse eficientemente. Las fuerzas de seguridad intentan mantener el orden, pero la falta de coordinación y la creciente frustración de la población complican la situación. Las colas en los bancos se vuelven interminables y muchos se quedan sin efectivo, ya que los cajeros automáticos no funcionan.

24 horas: Caos total

Después de 24 horas, el impacto en la sociedad es devastador. La vida moderna, dependiente de la tecnología digital, queda reducida a un caos total. Los hospitales, sin acceso a sistemas electrónicos, deben **recurrir a procedimientos manuales**. Los servicios de transporte y logística se paralizan, lo que afecta a la distribución de alimentos y medicinas. Las comunicaciones entre gobiernos y organismos internacionales se complican, dificultando la gestión de crisis. La falta de información precisa genera confusión y pánico en la población.

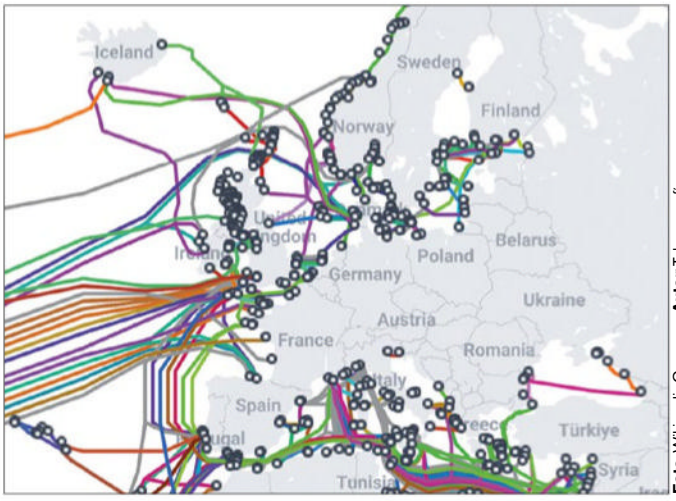


Foto: Wikimedia Commons **Autor:** Telegeografía

Mapa de los cables submarinos de comunicaciones que llegan a Europa. Estos cables son fundamentales para la conectividad global entre continentes.

Privilegiados con medios alternativos

Aunque la mayoría de la población queda aislada, algunos privilegiados disponen de medios alternativos para mantenerse conectados. Corporaciones, gobiernos y servicios de emergencia recurren a comunicaciones satelitales y redes privadas, pero incluso estos sistemas tienen limitaciones y no pueden sustituir la conectividad global de los cables submarinos.

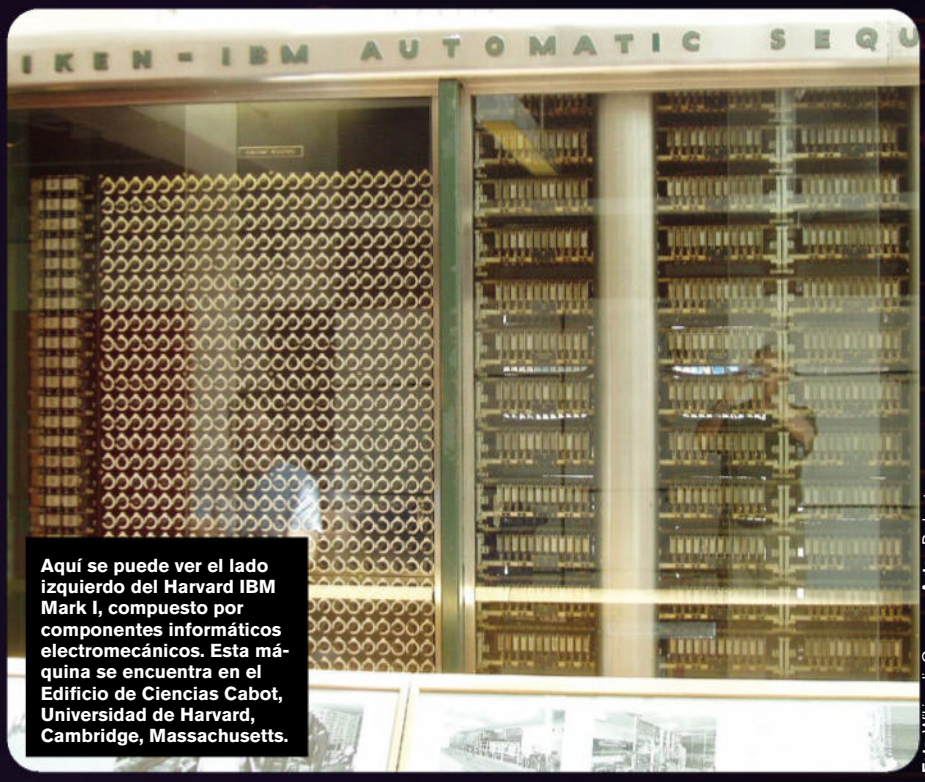
Un papel crucial lo juegan los radioaficionados que, con más de 3.500 operativos en España, se convierten en un valioso recurso para coordinar ayuda y transmitir información en situaciones de emergencia (Unión de Radioaficionados Españoles).

Demasiado frágiles

En conclusión, la interrupción global de Internet expondría la fragilidad de nuestra sociedad digital. La **dependencia de la red** para la mayoría de las actividades diarias, desde la economía hasta la seguridad, se haría evidente de manera alarmante.

Sin Internet, nuestra estructura social, económica y política quedaría desprotegida, lo que revela la necesidad de desarrollar infraestructuras de respaldo y estrategias de contingencia ante posibles escenarios de desconexión global.

Francisco José García Ull
Universidad Europea
theconversation.com



Aquí se puede ver el lado izquierdo del Harvard IBM Mark I, compuesto por componentes informáticos electromecánicos. Esta máquina se encuentra en el Edificio de Ciencias Cabot, Universidad de Harvard, Cambridge, Massachusetts.

Foto: Wikimedia Commons **Autor:** Daderot

Esta fotografía del Harvard IBM Mark I fue tomada en 2005 y muestra el extremo derecho de la máquina, que incluía lectores de datos, programas y sistemas automáticos para la escritura.

LA CURIOSA RAZÓN POR LA QUE LLAMAMOS 'PARCHES' A LAS CORRECCIONES DE BUGS

Cada día descargamos actualizaciones de aplicaciones que se encargan de corregir errores y mejorar su rendimiento. Pero ¿por qué llamamos 'parche' a este tipo de correcciones?

Los 'parches', en términos informáticos, tienen casi 80 años de edad. Su uso original quedó desterrado hace décadas con el auge de las nuevas tecnologías, pero se ha mantenido el término. Así, los parches de software se estrenaron en **1944** con el ordenador electromecánico **IBM Harvard Mark I**.

En cualquier caso, su origen en muy curioso. 'Parche', es una palabra muy descriptiva.: ponemos un parche en un agujero de la ropa para taparlo... y eso es justo lo que hacen los parches informáticos, pero con el software. Sin embargo, su adopción no tiene nada que ver con la vestimenta; es todo más literal.

¿De dónde provienen los parches informáticos?

El ordenador Mark I fue creado por IBM y la Universidad de Harvard en 1944. Era un modelo electromecánico **inspirado en la máquina de Babbage** (uno de los primeros ordenadores de la historia), que aún usaba botones, palancas y engranajes. El Mark I tenía 760.000 ruedas y 800 km de cable, un auténtico monstruo de 15,5 m de largo, un peso de 5 t, unos 2,40 m de alto y aproximadamente 60 cm de ancho. Además, era muy lento al realizar su trabajo, ya que tardaba entre 3 s y 5 s en completar una operación matemática, pero en realidad eso era un prodigio para la época.

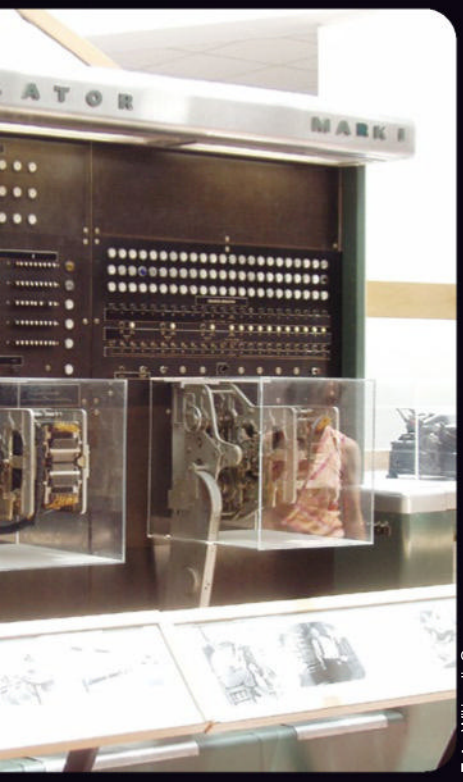
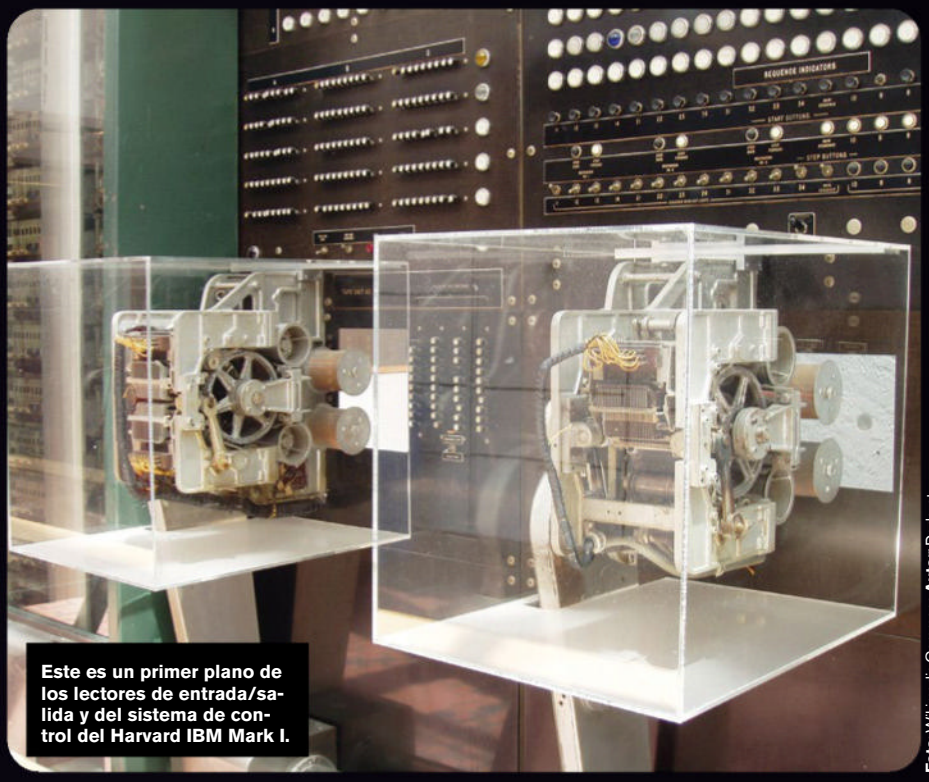


Foto: Wikimedia Commons



Este es un primer plano de los lectores de entrada/salida y del sistema de control del Harvard IBM Mark I.

Foto: Wikimedia Commons **Autor:** Daderot

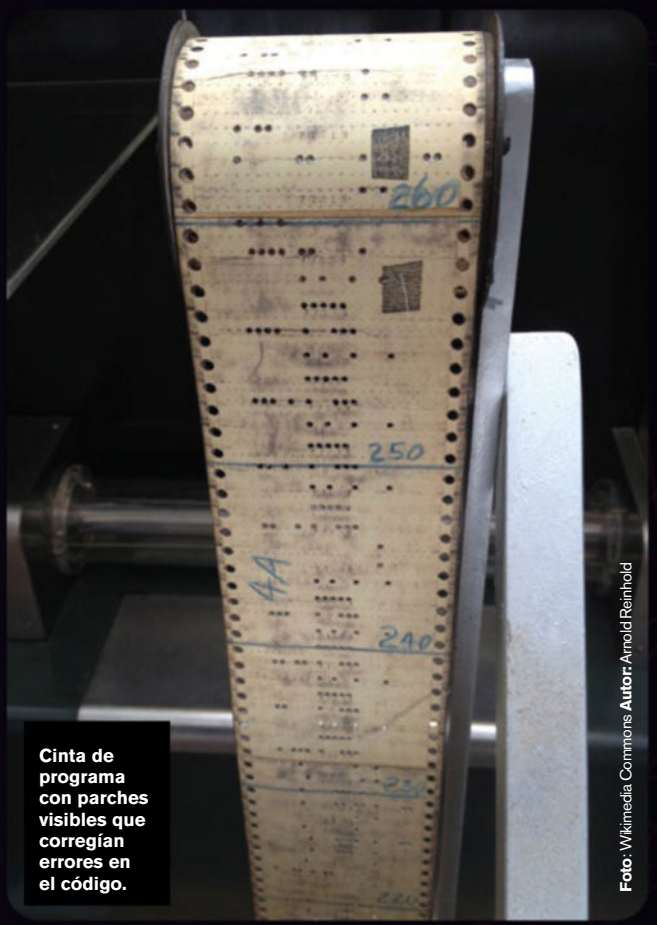
El Mark I utilizaba cintas perforadas para almacenar datos y aplicaciones. Estas cintas de papel **se enrollaban sobre sí mismas**, de forma parecida a las cintas de casete o los rollos de las películas de cine. No obstante, eran mucho más grandes.

Las cintas perforadas utilizaban agujeros cuya posición representaba un bit o una instrucción, según su posición. Sí, ya nos estamos acercando al origen del término 'parche'... ¿lo adivinas? Desde los inicios del software, han existido los bugs. Así, cuando los programadores detectaban un error en una aplicación almacenada en cinta perforada, debían encontrar la manera de poder corregirlo.

El historiador informático Dave Farquhar explica que el término 'parche' tiene un origen literal. Es decir, cuando se detectaba un error en la cinta perforada, lo cubrían con un trozo de papel o cinta adhesiva y, seguidamente, perforaban la corrección. En algunos casos, el parche era más grande que el fallo original, lo que obligaba a cortar la cinta y unir los extremos con la parte corregida. Así nació el concepto 'parchear un programa', algo que ha perdurado durante casi 80 años.

Sin embargo, aquí no queda todo, después de las cintas llegaron las tarjetas perforadas, que mantenían el mismo concepto pero eran más fáciles de manejar. Fue en los años 70 cuando comenzaron a utilizarse **disquetes, cintas magnéticas y discos duros**, desechando para siempre el papel perforado.

Han pasado 50 años desde que el término 'parche' dejó de tener un significado literal en la informática, pero aún lo usamos por tradición para referirnos a actualizaciones de software que corrigen bugs. Incluso en el mundo tecnológico, donde lo innovador rápidamente queda obsoleto, algunas costumbres perduran en el tiempo.



Cinta de programa con parches visibles que corregían errores en el código.

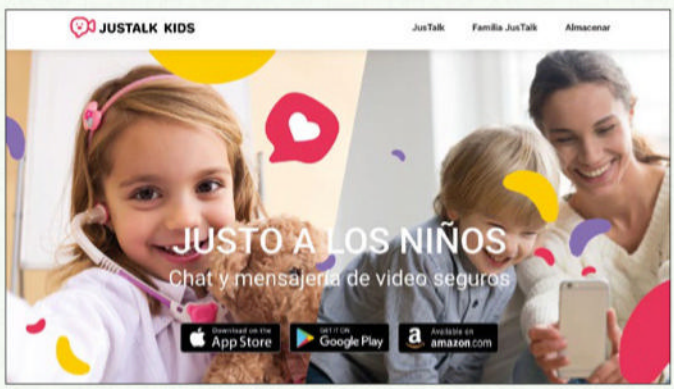
Foto: Wikimedia Commons **Autor:** Arnold Reinhold

¿CUÁNDO Y CÓMO?

NIÑOS Y GRUPOS DE

Esta situación es más que probable en una casa en la que vive un niño o niña de **alrededor de 11 años**. El preadolescente llega de la escuela y pide a sus padres que se unan al grupo de WhatsApp porque todos sus amigos están allí. La edad media de uso del teléfono móvil en España se sitúa en los 10,84 años. La presión social para tener uno desde una edad temprana es real, pero ¿es en realidad una buena idea?

Algunas de las principales aplicaciones de mensajería y redes sociales, como WhatsApp, Instagram o TikTok, sitúan dentro de sus términos y condiciones de uso la edad mínima de 13 años para crear una cuenta (aunque todas ellas están sujetas a las políticas de cada país: en Corea del Sur es de 14 años y en España se prevé que ascienda hasta los 16). A pesar de esto, muchos niños se registran antes, a veces **sin el conocimiento o permiso de los adultos**, para evitar sentirse aislados.



JusTalk Kids es una app segura de videollamadas y mensajes, diseñada para que los niños se comuniquen solo con personas de confianza.

Antes de decidir si un niño debe usar WhatsApp por motivos prácticos o sociales, es fundamental evaluar si es la mejor alternativa a pesar de las buenas intenciones. Existen aplicaciones de redes sociales y mensajería especialmente enfocadas en la infancia, como es el caso de **Zigazoo o JusTalk Kids Messenger**, a través de las que se pueden reducir los numerosos riesgos para los menores dentro de WhatsApp y otras plataformas.

Vulnerabilidad y supervisión

Los estudios muestran que el uso de teléfonos celulares sin una supervisión parental cuidadosa aumenta el riesgo de acoso cibernético, uso problemático y conductas perjudiciales para el desarrollo social.

Entre los 10 y los 16 años, los menores son especialmente vulnerables a la presión de grupo, a la impulsividad y a los riesgos para su autoestima. Aunque algunos preadolescentes de 13 años son muy ma-

WHATSAPP

Los expertos aconsejan a los padres supervisar qué hacen los menores en su tiempo libre, para evitar que la tecnología se convierta en un problema.

duros y otros de 17 aún no, la decisión debe basarse en la madurez del menor, su autocontrol y su capacidad para **manejar conflictos y rechazos**, así como la influencia de sus pares.

Qué debemos saber

Antes de permitir el acceso, es fundamental preparar a los menores para que su primera experiencia en los grupos de mensajería sea positiva y segura. En cualquier caso, este aprendizaje debe comenzar en la familia y continuar en la escuela.

Se recomienda que los padres supervisen el uso digital, accediendo a contraseñas y revisando mensajes y contactos, explicando los motivos.

Enseñar las reglas de la llamada netiqueta es esencial: así como aprendemos a interactuar con respeto y cortesía en persona, también debemos aprender a mantener **conversaciones respetuosas en el entorno digital**, donde la empatía y la intención del mensaje pueden ser más difíciles de percibir.

¿Qué se puede y qué no se debe compartir?

Además, es necesario establecer reglas claras y consensuadas sobre el tiempo de uso y qué se puede compartir, con quién y cuándo. Es necesario enseñarles a no compartir información personal, fotos privadas o información relacionada sobre su ubicación o hábitos.

Otro aprendizaje esencial es practicar la respuesta (o no respuesta) a mensajes hirientes, bromas o exclusiones, y reaccionar a mensajes ofensivos o perturbadores. Estos aprendizajes no son puntuales, sino que requieren un apoyo continuo, a medida que las situaciones evolucionan a lo largo de la adolescencia.

¿Cómo realizar la supervisión digital?

Supervisar no significa espiar ni prohibir, sino apoyar activamente y progresivamente. Es importante crear una cultura familiar y escolar que priorice la **comunicación presencial** y el tiempo libre por encima de

los intercambios virtuales y que reserve tiempos sin teléfonos móviles. La clave es adaptar el nivel de control a la edad y **madurez del niño**, manteniendo un diálogo abierto.

Durante los primeros años, se recomienda que los padres tengan acceso a las contraseñas y revisen periódicamente los mensajes, y expliquen previamente los motivos de esas revisiones partiendo de una colaboración con el niño. Los controles parentales permiten limitar el tiempo y el uso de contenido, y garantizar la privacidad y la seguridad. Esto también posibilita la revisión de contactos y grupos para que los menores puedan abandonar aquellos con los que no se sienten cómodos.

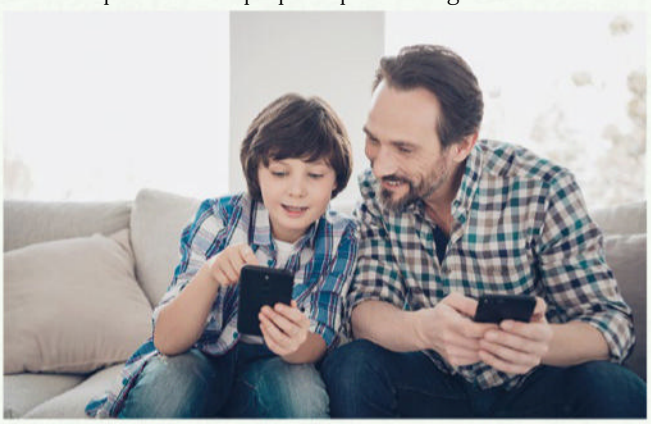
Una buena práctica a seguir es fomentar la participación de forma gradual: comenzar solo con grupos familiares o amigos muy cercanos y luego **ampliar gradualmente el círculo** a medida que demuestren responsabilidad y madurez.

Foto: Depositphotos.com

Según los expertos, la prohibición total de la tecnología a los niños puede llegar a ser contraproducente. La clave parece situarse en un término medio, con la supervisión de los padres en las edades más tempranas.

Los controles parentales permiten limitar el tiempo y el uso de contenido, y garantizar la privacidad y la seguridad

El ejemplo de los adultos es un elemento clave: los padres deben supervisar su propio uso del teléfono celular y modelar cómo gestionar los conflictos y la privacidad digital.



El acompañamiento activo implica conocer a los amigos y actividades del menor, guiando el uso de Internet con presencia y diálogo.

¿Durante cuánto tiempo se debe supervisar?

No existe una edad concreta para finalizar la supervisión, pero sí algunos indicadores: cuando el menor demuestra responsabilidad, sabe pedir ayuda, respeta las normas y gestiona bien los conflictos, el seguimiento puede ser más discreto. Sin embargo, la adolescencia es un período particularmente vulnerable. Por ello, conviene continuar con la supervisión, incluso de una forma menos intrusiva, al menos hasta los 16 años.

Entre los 13 y los 16 años, edad legal para el uso de mensajes personales y redes sociales, se recomienda lo siguiente:

- **Acompañamiento activo:** conocer las actividades, amistades y preocupaciones del menor, mostrando afecto y apoyo. Los adultos deben estar presentes durante el acceso a Internet y el uso de dispositivos, guiando y explicando los posibles riesgos existentes y las buenas prácticas.
- **Control de contenidos:** filtrar y limitar el acceso a contenidos que sean inapropiados, restringir la instalación de aplicaciones y la participación en redes sociales o grupos de mensajería.
- **Establecimiento de rutinas:** pactar horarios y tiempos de uso, y fomentar actividades fuera de las pantallas.
- **Educación en habilidades digitales:** enseñar a identificar situaciones de riesgo y a pedir ayuda ante cualquier problema que pueda surgir.

Más adelante, aunque la supervisión se reduzca, los adultos deben seguir siendo referentes, estar disponibles para resolver dudas o problemas y atentos a señales de riesgo como adicción, aislamiento o conductas problemáticas.

En definitiva, la decisión sobre cuándo se puede permitir el acceso a grupos de mensajería debe basarse en la madurez del menor, la supervisión activa y el acompañamiento continuo, priorizando siempre la seguridad y el bienestar emocional.

Ana Cebollero Salinas,
Carmen Elboj,
Pablo Bautista Alcaine,
Tatiana Íñiguez Berrozpe
Universidad de Zaragoza
theconversation.com

EVITA VIRUS Y ESTAFAS

COSAS QUE JAMÁS DEBERÍAS BUSCAR EN GOOGLE

SEO Poisoning es una técnica utilizada por los delincuentes para promocionar páginas maliciosas desde las que insertar malware en los equipos de los usuarios.

Como la charca de agua a la que todos los animales van a beber, el buscador de Google es el coto de caza de los depredadores en la Red, los ciberdelincuentes. Los expertos revelan ahora cinco tipos de búsquedas en Google que te pueden redirigir directamente a webs y **sitios de descarga infectados**.

El 90 % de los usuarios de Internet utiliza Google como su principal herramienta para localizar información, algo que los hackers han aprendido a explotar mediante una técnica conocida como SEO Poisoning o Envenenamiento por SEO. Esta estrategia consiste en identificar las búsquedas 'desesperadas' o de alta urgencia, más susceptibles a captar clics, para redirigir a los usuarios a sitios web maliciosos con el objetivo de robar sus datos o instalar troyanos en sus equipos.

Así funciona la técnica

SEO Poisoning consiste en aprovechar las técnicas de posicionamiento en los motores de búsqueda (SEO) para situar una página web maliciosa entre los primeros resultados de Google. Los ciberdelincuentes diseñan así sitios fraudulentos relacionados con búsquedas urgentes, aprovechándose de la predisposición de los usuarios a **hacer clic en los primeros enlaces**. Jake Moore, asesor global de ciberseguridad en ESET, destaca en Daily Mail cinco tipos de búsquedas potencialmente peligrosas en Google diseñadas para robar información personal o instalar malware.

- **Números de teléfono de soporte técnico:** al buscar el teléfono de empresas conocidas, a veces aparecen números falsos que te ponen en contacto con un estafador. Este se hará pasar por un representante oficial de la compañía e intentará convencerte para que le entregues tus datos personales, la información de tu tarjeta de crédito, tus claves y otros datos personales. Para evitar esta estafa, hay que buscar los números directamente en la web de la empresa.
- **Búsquedas relacionadas con dinero rápido:** frases como 'préstamos fáciles', 'formas rápidas de ganar dinero' o 'trabajos remotos bien pagados' son un gancho habitual. Los ciberdelincuentes diseñan webs falsas que ofrecen préstamos con un bajo interés, o trabajos remotos que están muy bien pagados. Sin embargo, antes de que obtengas el dinero o salario, te pedirán tus datos personales, bancarios o de tarjetas de crédito, que luego utilizarán para cometer delitos. Desconfía de ofertas demasiado buenas y confirma siempre la fuente.
- **Google Authenticator:** aunque su uso ha disminuido por el auge de las passkeys, hasta hace poco tiempo esta aplicación de Google era imprescindible para abrir una cuenta en muchos servicios, y hoy día sigue siendo muy demandada. Según Malwarebytes, al buscarla en Google, pueden aparecer webs falsas que, mediante phishing, simulan ser la web oficial de descarga. Estas páginas distribuyen malware que infectará tu ordenador con software diseñado para robar contraseñas. Para evitar esto, descarga solo apps desde tiendas oficiales.
- **Compras de 'viagra' o similar:** investigadores de SolidVIP han identificando una táctica en la que los delincuentes se infiltran en sitios farmacéuticos o blogs vulnerables, sobre todo en aquellos basados en WordPress, e insertan enlaces fraudulento en los anuncios de venta. Luego, cuando el comprador hace un pedido, no lo recibe u obtiene un producto falso.
- **Cuestionarios sobre 'fortaleza mental deportiva':** la empresa de seguridad Menlo Security descubrió una extraña búsqueda maliciosa relacionada con cuestionarios deportivos que pueden redirigirte a PDF infectados. Estos, al abrirse, descargan malware automáticamente sin que el usuario lo sepa: desde virus para robar identidad hasta ransomware para bloquear el acceso a los datos del usuario. Este peligro se extiende a cualquier búsqueda que implique la descarga de ficheros PDF en una fuente desconocida, así que evita acciones de este tipo. ■

AVANCE

A LA VENTA EL 29 DE AGOSTO

ESPECIAL CENTRO DE DESCARGAS

DESCUBRE EL PODER DE LAS APPS GRATUITAS

¿Sabías que hay herramientas gratuitas que pueden facilitarte la vida digital? Desde editar fotos hasta navegar de forma más eficiente o mejorar tu productividad, en Internet abundan programas útiles y accesibles para todos. En el próximo número, te ofrecemos una selección de estas aplicaciones, con explicaciones sobre cómo funcionan y en qué tareas pueden ayudarte.

CONTRAATAQUE

LO MÁS NUEVO DE SAMSUNG

Samsung fue pionero en relojes inteligentes y móviles plegables, pero se enfrenta a una dura competencia. Con nuevos modelos, busca recuperar su liderazgo.

NORMATIVA UE

¿EL FIN DE LOS MÓVILES BARATOS?

Una nueva normativa de la UE exige móviles más duraderos, seguros y actualizables, lo que plantea importantes retos e implicaciones para fabricantes y consumidores.

LUMMA STEALER

GOLPE CONTRA EL ROBO DIGITAL

Microsoft, ESET y socios internacionales desmantelaron la red cibercriminal Lumma Stealer, especializada en robar datos como contraseñas y cuentas bancarias. Tras meses de vigilancia técnica y coordinación legal, lograron tomar el control de los servidores, desactivar la infraestructura y desorganizar a los ciberdelincuentes.

Computer Hoy

Práctica · Actual · Quincenal

Redactor Jefe
Carlos Gombau
carlos.gombau@henneo.com

Jefa de Sección
Fuencisla Mira
fuencisla.mira@henneo.com

Director de Arte
Abel Vaquero
abel.vaquero@henneo.com

Maquetación
Paula Cuesta

Colaboradores
Óscar Díaz, Tomás González, Ana Abad y Luis Sanz

Contacto redacción
computerhoy@henneomagazines.com

Fotografía
Depositphotos y Getty Images

Publicidad - Alayans
Director General: Jesús Aspra
Equipo comercial: Marianela Ruiz y Alejandro Fuertes

Contacto suscripciones
Tel. +34 915 140 600
suscripciones@henneomagazines.com

HENNEO MAGAZINES, S.A.
C/ Canarias, 49, 28045 Madrid
Tel. +34 915 140 600

Una publicación de
HENNEO

Presidente
Fernando de Yarza López-Madrazo
Consejero Delegado
Íñigo de Yarza López-Madrazo
Director Editorial y de Comunicación
Miguel Ángel Liso Tejada

Imprime
Gráficas Jomagar, SL

Queda prohibida la reproducción total o parcial, por cualquier medio o en cualquier soporte de los contenidos de esta publicación sin el permiso previo y por escrito del editor.

De acuerdo con lo establecido en la normativa sobre Protección de Datos de Carácter Personal, te informamos que tus datos serán tratados por el Responsable del tratamiento Henneo Magazines S. A. y que se utilizarán para (i) gestionar las consultas, análisis y opiniones que nos envíes, (ii) gestionar tu participación en el sorteo o concurso y el envío del premio, (iii) analizar los datos aportados en las encuestas que hayas completado voluntariamente (iv) y ofrecerte, mediante el envío de comunicaciones comerciales, productos o servicios de nuestra propia empresa o de terceros relacionados con los sectores editorial, automoción, informática, tecnología, telecomunicaciones, electrónica, videojuegos, seguros, financiero y crédito, infancia y puericultura, alimentación, formación y educación, hogar, salud y productos farmacéuticos, ocio, gran consumo, cuidado personal, agua, energía y transportes, turismo y viajes, inmobiliario, juguetería, textil, ONG y productos/servicios para animales y mascotas. La base legitimadora del tratamiento es tu consentimiento. Tus datos no serán cedidos a terceros, excepto cuando sean publicados en nuestra revista para dar a conocer la respuesta a tu consulta, tu opinión, análisis o la relación de ganadores del concurso, garantizando la transparencia.

Los datos personales proporcionados serán conservados hasta que sea necesario para cumplir con la finalidad descrita o hasta la retirada del consentimiento.

Podrás ejercitar tus derechos de acceso, rectificación, portabilidad, supresión, limitación del tratamiento, retirada del consentimiento y oposición mediante escrito a Henneo Magazines S. A., C/ Canarias 49, 28045, Madrid o correo electrónico a **dpo@henneomagazines.com**.

Este sumario puede modificarse por exigencias de la actualidad. En ese caso, confiamos en vuestra comprensión.

¡Nueva!

Computer Hoy

Oferta de suscripción

Bitdefender

Digital Identity Protection

La protección que escanea la web en busca de filtraciones no autorizadas de **tus datos personales**, monitorea si tus cuentas están expuestas y facilita la adopción de medidas mucho antes de que ocurra un desastre. PVP recomendado: **69,99€/año**

por sólo **59€**

~~160,99€~~

Sin gastos de envío

+ 26 números de Computer Hoy

Puedes suscribirte por cualquiera de estos canales:

https://www.henneomagazines.com/collections/suscripciones-computer-hoy

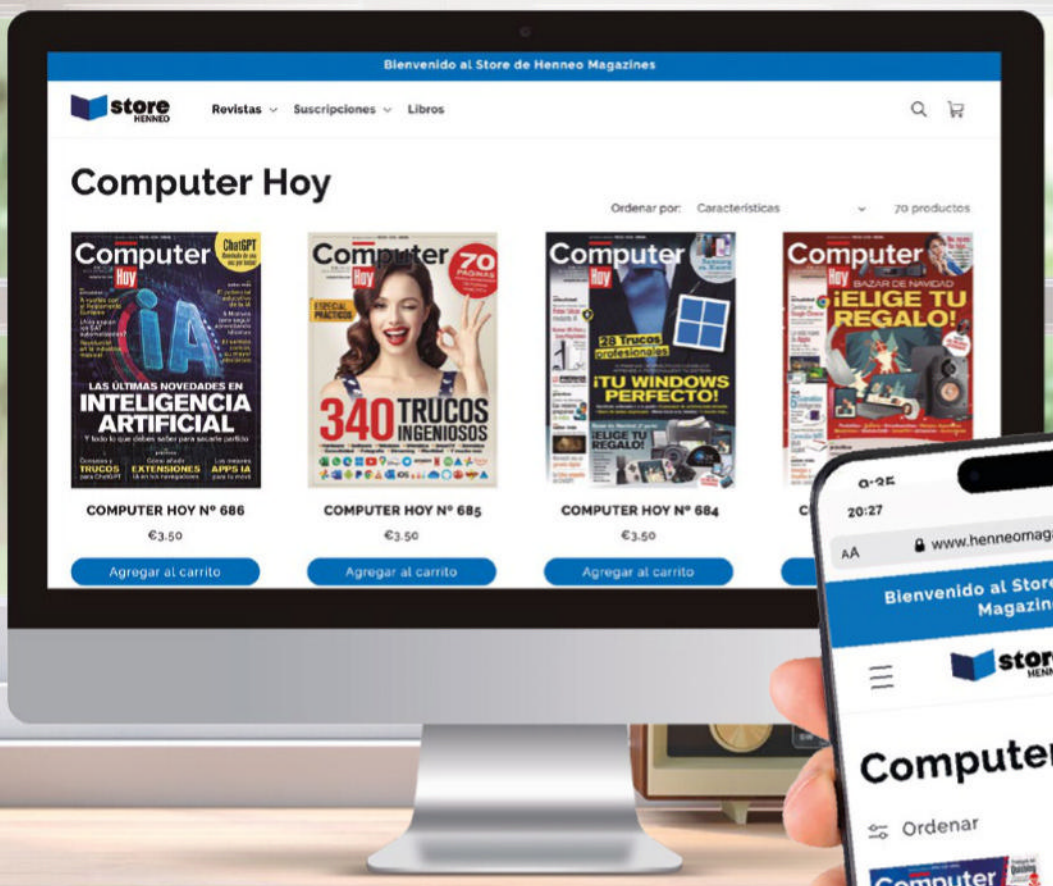
Por teléfono: 915 140 600 / **Por email:** suscripciones@henneomagazines.com

Cada suscriptor tendrá acceso gratuito a la edición digital de Computer Hoy en Kiosko y Mas. Accesible desde PC, smartphones y tablets, con sistemas Windows 8, iOS y Android

En cumplimiento de la normativa vigente en materia de Protección de Datos personales, te informamos de que los datos que nos proporciones serán tratados por el Responsable del Tratamiento Henneo Magazines S.A. con objeto de (I) gestionar tu suscripción y (II) ofrecerte, mediante el envío de comunicaciones comerciales, productos o servicios de nuestra propia empresa o de terceros relacionados con los sectores editorial, automoción, informática, tecnología, telecomunicaciones, electrónica, videojuegos, seguros, financiero y crédito, infancia y puericultura alimentación, formación y educación, hogar, salud y productos farmacéuticos, ocio, gran consumo, cuidado personal, agua, energía y transportes, turismo y viajes, inmobiliario, juguetería, textil, ONG y productos/servicios para animales y mascotas. La base legitimadora del tratamiento es ejecución del contrato para la finalidad (I) e interés legítimo para la finalidad (II). Tus datos no serán cedidos a terceros, salvo obligación legal. Tus datos serán conservados hasta cumplir con la finalidad. Podrás ejercer tus derechos de acceso, rectificación, supresión, limitación del tratamiento y oposición mediante escrito a Henneo Magazines, S. A. C/Canarias 49, 28045 Madrid, o correo electrónico a computerhoy@henneomagazines.es.

store HENNEO

¿CONOCES NUESTRA TIENDA ONLINE?



- **Completa** tu colección Computer hoy
- **Suscríbete** a tu revista favorita
- **Descubre** ofertas especiales

Todo en **www.henneomagazines.com**